611-EMD-001

EOSDIS Maintenance and Development Project

Release 7 Mission Operation Procedures for the EMD Project

April 2004

Raytheon Company
Upper Marlboro, Maryland

Release 7 Mission Operation Procedures for the EMD Project

April 2004

Prepared Under Contract NAS5-03098
CDRL Item 23

RESPONSIBLE AUTHOR

Ralph E. Fuller /s/ 4/27/04

Ralph E. Fuller Date
EOSDIS Maintenance and Development Project

RESPONSIBLE OFFICE

Mary Armstrong /s/ 4/27/04

Mary Armstrong, Deputy Program Manager Date
EOSDIS Maintenance and Development Project

Raytheon Company
Upper Marlboro, Maryland

This page intentionally left blank.

Preface

This document is a formal contract deliverable. It requires Government review and approval within 45 business days. Changes to this document will be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office
The EMD Project Office
Raytheon Company
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5301

Revision History

Document Number	Status/Issue	Publication Date	CCR Number
611-EMD-001	Original	April 2004	04-0220

This page intentionally left blank.

Abstract

This document, Mission Operation Procedures for the EMD Project, provides DAAC procedures that assign and describe operators, engineers, operations support, administration and management staff actions required to configure, maintain and operate the ECS applications at maturity. The DAAC portion of this document contains system-level standard procedures that can be modified at the DAACs during subsequent training, operations exercises and procedure review activities to reflect desired uniqueness. The objectives of the current release of the system are to provide capability to support the ingest and archive of raw data obtained from instruments on Earth Observing System (EOS) satellites [e.g., the EOS AM Mission spacecraft 1, morning equator crossing spacecraft series (Terra (AM-1)), EOS PM Mission spacecraft 1, afternoon equator crossing spacecraft series (Aqua (PM-1)) and the Land Remote-Sensing Satellite (Landsat 7)]. Other capabilities provided by the current release include processing the data obtained, distributing raw or processed data as requested, quality assurance of processed data, supporting communication networks, and systems monitoring via interfaces with the ECS operations staff.

Keywords: operations, DAACs, SMC, EOC, mission support, operation procedures, EOS, Terra (AM-1), Aqua (PM-1), Aura, Landsat 7, software, integration, test, SSI&T, Version 0

This page intentionally left blank.

Contents

Preface

Abstract

1. Introduction

2. Related Documentation

3. System Administration

4. Database Administration

5. Security Services

6. Network Administration

7. System Monitoring

8. Problem Management Procedures

9. Configuration Management Procedures

10. Metadata Administration

11. Production Rules

12. Resource Planning

13. Production Planning

14. Production Processing

15. Quality Assurance

16. Ingest

17. Archive Procedures

18. Data Distribution

19. User Services

20. Library Administration

21. COTS Hardware Maintenance

22. Software Maintenance

23. Property Management

24. Installation Planning

25. COTS Training

26. Science Software Integration and Test (SSI&T)

27. Inventory Logistical Management (ILM)

28. Maintenance of Configuration Parameters

List of Figures

List of Tables

Appendix A. Additional Material

Abbreviations & Acronyms

1. Introduction

This document, Release 7 Mission Operation Procedures for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Maintenance and Development (EMD) Project, provides procedures to configure, maintain and operate the ECS system.

1.1 Identification

This document meets the milestone specified as Contract Data Requirements List (CDRL) Item 23, under contract NAS5-03098. It reflects the ECS as delivered at Release 7.

1.2 Scope

The scope of this document is directed to Distributed Active Archive Center (DAAC) operations activities to support the Release 7 ECS system. Both procedures and instructions are identified. Operations procedures are defined as the step-by-step commands or on-line procedures needed to perform a function. The Operations Instructions are the off-line procedures or directives for performing administrative, operations, management, or operations support activities (e.g., Configuration Management, Problem Management, Quality Assurance).

1.2.1 On-Site Procedures Tailoring Guide

Each DAAC may modify these procedures and instructions to accommodate site-specific operations requirements. Such documentation should be versioned and dated in MS Word format with a master copy forwarded to the following address:

EMD Training
The EMD Project Office
Raytheon Company
1616 McCormick Drive
Upper Marlboro, MD 20774-5301

For specifics on authoring, formatting, importing, exporting and maintenance of procedures and instructions see Chapter 20, Library Administration.

1.3 Purpose

The purpose of this document is to identify the procedures and instructions to operate and maintain Release 7 systems. In addition, DAAC staff responsibilities are identified. The DAAC operations staff is comprised of operators, engineers, as well as operations support, administration and management staff personnel.

This document will also be used as a training aid for operations staff who are located at the sites. The operations procedures and operations instructions were derived from, and are intended to be consistent with, the system functions and capabilities specified in the ECS design specifications and the operations activities described in the ECS Operations Concept Document.

1.4 Status and Schedule

This document is to be delivered with each Release of ECS. Updates will be made to reflect subsequent system releases. Changes will be submitted through established configuration management procedures, such as document change notices or published revisions known as interim updates published to the web site at http://edhs1.gsfc.nasa.gov/ at an "Interim Updates" link on the abstract page for this document (611-EMD-001).

1.5 Organization

The contents subsequent to this first section are presented as follows:

- Section 2 **Related Documentation.** Lists documents that drive, support or expand on the material in this manual.
- Section 3 **System Administration.** Identifies the operations procedures and/or operations instructions for system administration activities, such as backup and restore, log maintenance, user account administration, and workstation installation.
- Section 4 **Database Administration.** Identifies the operations procedures and/or operations instructions for database administration activities, such as product installation, disk storage management, login and privileges administration, database validation, backup and recovery, database configuration, tuning and performance monitoring.
- Section 5 **Security Services.** Identifies the operations procedures and/or operations instructions for security services activities, such as user authentication and authorization, data access control, network services monitoring, password protection, file modification monitoring.
- Section 6 **Network Administration.** Identifies the operations procedures and/or operations instructions for network administration activities, such as network and system configuration monitoring, network services monitoring.
- Section 7 **System Monitoring.** Identifies the operations procedures and/or operations instructions for network system monitoring, such as problem monitoring and resolution.
- Section 8 **Problem Management.** Identifies the operations procedures and/or operations instructions for submitting trouble tickets and for processing and resolving trouble ticket submissions.

- Section 9 **Configuration Management.** Identifies the operations procedures and/or operations instructions for configuration management activities, such as Configuration Control Board (CCB) support, configuration item identification, submission and processing of configuration change requests (CCRs), configuration status accounting, configuration audits, data management, operational database maintenance, software transfer and installation.
- Section 10 **Metadata Administration.** Identifies the operations procedures and/or operations instructions for metadata administration activities, such as establishing collections, populating the database, and specifying Earth Science Data Type (ESDT) services.
- Section 11 **Production Rules.** This section is intended to explain the production rules governing the use of product generation executives (PGEs) in ECS. This section addresses the syntax for specifying production rules.
- Section 12 **Resource Planning.** Identifies the operations procedures and/or operations instructions for resource planning activities for non-production (ground) events.
- Section 13 **Production Planning.** Identifies the operations procedures and/or operations instructions for production planning activities for production jobs, resource prioritization, and scheduling.
- Section 14 **Production Processing.** Identifies the operations procedures and/or operations instructions to support data processing activities.
- Section 15 **Quality Assurance.** Identifies the operations procedures and/or operations instructions to perform DAAC manual non-science quality assurance activities, such as visualization of science data products and updating quality assurance metadata.
- Section 16 **Ingest.** Identifies the operations procedures and/or operations instructions to support data acquisition.
- Section 17 **Archive Procedures.** Identifies the operations procedures and/or operations instructions for archiving activities, such as archive repository maintenance, fault monitoring and notification, and temporary data storage.
- Section 18 **Data Distribution.** Identifies the operations procedures and/or operations instructions to support data distribution activities, such as media operations and product shipment (including Product Distribution System operations).
- Section 19 **User Services.** Identifies the operations procedures and/or operations instructions to support user services activities to address user requests for data.

- Section 20 **Library Administration.** Identifies the operations procedures and/or operations instructions to support librarian administration activities, such as change package preparation and distribution, master document control and maintenance.
- Section 21 **COTS Hardware Maintenance.** Identifies the operations procedures and/or operations instructions for preventive and corrective maintenance activities of commercial off-the-shelf (COTS) hardware for the ECS project.
- Section 22 **Software Maintenance.** Identifies the operations procedures and/or operations instructions to support maintenance activities for COTS software, custom software, and science software.
- Section 23 **Property Management.** Identifies the operations procedures and/or operations instructions for the receipt, control, and accountability of ECS property at ECS sites.
- Section 24 **Installation Planning.** Identifies the operations procedures and/or operations instructions to support installation planning activities for conducting site surveys, ensuring that site preparations/coordination are completed on schedule, facilitating receipt and installation of the hardware.
- Section 25 **COTS Training.** Identifies the operations procedures and/or operations instructions to support COTS training activities, such as training request processing, training coordination, training scheduling, and training record maintenance.
- Section 26 **Science Software Integration and Test (SSI&T).** Identifies the operations procedures and/or operations instructions to support science software integration and test activities.
- Section 27 **Inventory Logistical Management (ILM).** ILM helps the operations staff at the DAACs, EOC, and SMC to maintain records that describe all inventory components and their assembly structures and interdependencies. The database maintained by this tool, keeps chronological histories (a record of the transactions) of receipt, installation, and relocation of inventory items. There is a license management section and general updates to work order processes, forms, and report formats.
- Section 28 **Maintenance of ECS Configuration Parameters.** These procedures describe the overall maintenance of the ECS Configuration Parameters Baseline for ECS custom software and hardware, including patches, database, operating systems, COTS software, and networks.
- Appendix A **Additional Material.** Contains examples of Object Description Language (ODL) files used by various instrument teams, to illustrate concepts discussed in Section 26.

- **Abbreviations and Acronyms.** Identifies abbreviations and acronyms used throughout this document.

This page intentionally left blank.

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which the Mission Operation Procedures' scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-46-03	EMD Task 101 Statement of Work For ECS SDPS Maintenance
423-46-02	Contract Data Requirements Document for EMD Task 101 ECS SDPS Maintenance

2.2 Applicable Documents

The following documents are referenced within the Mission Operation Procedures document, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) (ECS F&PRS)
423-46-01	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Science Data Processing System (EMD F&PRS)

2.3 Information Documents

2.3.1 Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

104-EMD-001	Software Quality Assurance Plan for the EMD Project
105-EMD-001	Property Management Plan for the EMD Project
110-EMD-001	Configuration Management Plan for the EMD Project

302-EMD-001	Software Maintenance and Development Plan for the EMD Project
313-EMD-001	Release 7 ECS Internal Interface Control Document for the EMD Project
500-EMD-001	Terra Spacecraft Ephemeris and Attitude Data Preprocessing
500-EMD-002	Aqua Spacecraft Ephemeris and Attitude Data Preprocessing
500-EMD-003	Aura Spacecraft Ephemeris and Attitude Data Preprocessing
609-EMD-001	Release 7 Operations Tools Manual for the EMD Project
910-TDA-022	Custom Code Configuration Parameters for ECS

2.3.2 Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

303-EMD-001	Hardware Maintenance and Development Plan for the EMD Project
305-EMD-001	Release 7 Segment/Design Specification for the EMD Project
311-EMD-001	Release 7 Data Management Subsystem (DMS) Database Design and Database Schema Specifications for the EMD Project
311-EMD-002	Release 7 INGEST (INS) Database Design and Schema Specifications for the EMD Project
311-EMD-003	Release 7 Planning and Data Processing Subsystem Database Design and Schema Specifications for the EMD Project
311-EMD-004	Release 7 Science Data Server Database Design and Schema Specifications for the EMD Project
311-EMD-005	Release 7 Storage Management and Data Distribution Subsystems Database Design and Database Schema Specifications for the EMD Project
311-EMD-006	Release 7 Subscription Server Database Design and Schema Specifications for the EMD Project
311-EMD-007	Release 7 Systems Management Subsystem Database Design and Schema Specifications for the EMD Project
311-EMD-008	Release 7 Registry Database Design and Schema Specifications for the EMD Project
311-EMD-009	Release 7 Product Distribution Subsystem (PDS) Database Design and Database Schema Specifications for the EMD Project

311-EMD-010	Release 7 NameServer Database Design and Schema Specifications for the EMD Project
311-EMD-011	Release 7 Order Manager Server Database Design and Schema Specifications for the EMD Project
311-EMD-012	Release 7 Spatial Subscription Server Database Design and Schema Specifications for the EMD Project
311-EMD-013	Release 7 Data Pool Database Design and Schema Specifications for the EMD Project
503-EMD-001	Release 7.0 Transition Plan for the EMD Project
152-TP-001	ACRONYMS for the EOSDIS Core System (ECS) Project
152-TP-003	Glossary of Terms for the EOSDIS Core System (ECS) Project

This page intentionally left blank.

3. System Administration

This section covers the procedures necessary for the System Administrator (SA) and/or Operator (OPR) to manage and operate the system.

Detailed procedures for tasks performed by the System Administrator and/or Operator are provided in the sections that follow. The procedures assume that the administrator and/or operator is authorized and has proper access privileges to perform the tasks (i.e., root) and that the SA and/or OPR has been properly trained in all aspects of the system.

Each procedure outlined will have an **Activity Checklist** table that will provide an overview of the task to be completed. The outline of the **Activity Checklist** is as follows:

Column one - ***Order*** shows the order in which tasks should be accomplished.

Column two - ***Role*** lists the Role/Manager/Operator responsible for performing the task.

Column three - ***Task*** provides a brief explanation of the task.

Column four - ***Section*** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - ***Complete?*** is used as a checklist to keep track of which task steps have been completed.

The following is the **Activity Checklist** table that provides an overview of the overall system administration processes and who performs them

Table 3-1. System Administration - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPR	Secure Shell	(I) 3.1	
2	OPR	System Startup/Shutdown	(I) 3.2	
3	OPR	System Backup and Restore	(I) 3.3	
4	SA	User Administration	(I) 3.4	
5	SA	Security	(I) 3.5	

For procedures outlined in this section, there are corresponding **QUICK STEP** procedures immediately following in this chapter. The **QUICK STEP** procedures are designed for persons who have ***prior training or are experienced system administrators with prior system administration experience.*** The ***QUICK STEP*** procedures should be used by ***experienced persons ONLY***.

3.1 Secure Shell

Secure Shell (ssh) is a set of programs that greatly improve network security. The primary need for it on ECS is to allow secure, interactive access to ECS DAACs without needing burdensome procedures and mechanisms and additional hardware.

Secure in this context means not sending passwords "in the clear" so that hackers may intercept them and also provides encryption of the entire session.

Secure Shell is to be used for any inter-access among system platforms and between DAACs

Table 3.1-1. Secure Shell - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS	Initiating sshsetup	(I) 3.1.1	
2	OPR	Setting up remote access ssh	(I) 3.1.2	
3	OPR	Changing Your Passphrase	(I) 3.1.3	

3.1.1 Setting Up ssh

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing ssh commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via ssh. The process is started by running the sshsetup script which will enable ssh to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

To initialize Secure Shell Access (ssh), execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup**, then press Return/Enter.

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

```
Initializing random number generator...
Generating p:  Please wait while the program completes ...
%
```

- This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.

3.1.2 Remote ssh Access

If you need to access a host with a different home directory, you will need to run the sshremote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

To set up remote access shell (ssh), execute the procedure steps that follow:

1 Login into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote**, then press Return/Enter.

- You will see the following prompt:

```
You have a local passphrase. Do you want to setup for:
1  VATC
2  EDF
3  MiniDAAC
4  GSFC DAAC
5  SMC
6  GSFC M and O
7  EDC DAAC
8  EDC M and O
9  LaRC DAAC
10  LaRC M and O
11  NSIDC DAAC
12  NSIDC M and O
x  Exit from script
Select:
```

3 At the "Select" prompt, type in the corresponding number to the desired host, then press Return/Enter.

- You will receive a prompt similar to the following for the VATC:

```
Working...
```

4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** and then press Return/Enter.

- A prompt similar to the following will be displayed:

```
          Last login: Thu Jul  9 10:41:13 1998 from echuser.east.hit
                    No mail.
Sun Microsystems Inc.   SunOS 5.5.1     Generic May 1996
t1code1{username}1:
```

5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host

- You will see an information statement:

```
Use a passphrase of at least 10 characters which should include numbers
or special characters and MAY include spaces
```

6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

```
Initializing random number generator...
Generating p:  Please wait while the program completes ...
%
```

8 At the "t1code1" prompt type **exit**, the press Return/Enter.

- The following information will be displayed:

```
Updating locally...
Updating t1code1u.ecs.nasa.gov
 %
```

- This establishes the ssh key at the remote host and exchanges key information with your local host.

Note: The ssh keys at remote sites can be different from the local host ssh key.

3.1.3 Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The ssh keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

To change your Secure Shell Passphrase, execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **/tools/bin/sshchpass**, then press Return/Enter.
- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see an information prompt similar to the following:

```
ssh-keygen will now be executed. Please wait for the prompt to Return!
/home/bpeters/.ssh/authorized_keys permissions have already been set.

%
```

3.2 System Startup and Shutdown

The Startup and Shutdown processes begin when it has been determined by the DAAC Operations Supervisor or his designee that it is necessary to stop or start the system. The least impacting method is determined and users are appropriately notified.

When determining the least impacting way to perform the startup or shutdown, the OPR, along with the Operations Supervisor takes into consideration whether only specific server software packages would need to be started/stopped or an entire system startup/shutdown is required.

Once these steps have been taken, the shutdown or startup is performed.

The **Activity Checklist** table that follows provides an overview of the startup and shutdown processes.

Table 3.2-1. Startup/Shutdown - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS Sup	Determine that Startup/Shutdown is necessary.	(I) 3.2	
2	OPR	Determine the Least Impacting Way to Perform the Startup/Shutdown.	(I) 3.2	
3	OPR	Notify Those Effected by the Startup/Shutdown.	(I) 3.2	
4	OPR	Perform the Startup/Shutdown	(P) 3.2	

3.2.1 Startup

Startup means that power to the system is restored and the system is being taken to a fully useable and operational state.

3.2.1.1 Cold - By Subsystem

A cold startup means that power to the system has been previously powered off and the system(s) is being restarted from this cold state. The System Startup process begins after a previously completed shutdown, either scheduled or emergency. The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the SA.

This procedure assumes that the OPR has been properly trained to startup all aspects of the system and that the system is currently powered off (due to a normal or emergency shutdown).

The procedure assumes that the Startup has been scheduled well in advance, all planning involved has been concluded well in advance and all other Distributed Active Archive Centers (DAACs) have been notified of the system returning to an on-line state.

This section explains how to perform a cold system startup by subsystem. The sequence of the execution of the steps below are VERY IMPORTANT. To begin a cold system startup, execute the procedure steps that follow:

1 The **sequence** of booting the machines is **IMPORTANT**:

- ***Remember to power on peripherals before powering on each CPU***
- ***Monitor each system Boot Up activity on that system's monitor***
- ****The DNS and NIS servers must be booted FIRST***
- ***Once each system has booted without error, proceed to the next machine***
- Boot the machines per Table 3.2-2

2 Continue booting the remaining machines

Table 3.2-2 presents the cold system startup machine boot sequence, however, the machine names are to be added once identified at each DAAC, per their specific baseline by the SA.

Table 3.2-2. Cold System Startup - Machine Boot Sequence

Step	What to Enter or Select	Action to Take (Server)	Machine Name
1	(No entry)	NIS Master	**x0css02**
2	(No entry)	DNS Master	**x0css02**
3	(No entry)	Clearcase Server(s)	**x0mss0x**
	(No entry)	Interface Server(s)	**x0ins0x**
4	(No entry)	MSS	**x0mssxx**
5	(No entry)	DSS	**x0acs0x**
6	(No entry)	Ingest	**x0icg0x**
7	(No entry)	PDPS	**x0pls0x**
8	(No entry)	Others	

3.2.1.2 Warm - By Subsystem Startup

A warm startup means the system has been previously powered on, but the system(s) is not fully operational, either the system has had some service performed (i.e. single user mode) or is being rebooted to correct some minor malfunction. The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the software dependencies.

The order of the re-boot is contingent on software dependencies per site.

If the NIS server service has been interrupted, the users will automatically be transferred to a backup server. Once the faulty server(s) has been repaired, re-establish connection with the primary NIS server by rebooting the Backup Server; the users would then be transferred back to the primary NIS server.

Table 3.2-3 presents the **QUICK STEP** procedure required to perform a warm system startup.

Table 3.2-3. Warm System Startup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine software dependencies
2	(No entry)	reboot independent server(s)
3	(No entry)	reboot dependent server(s)

Note - in addition to warm system startup/reboot sequences, ECS servers which use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted, once the Sybase SQL server has come back on-line.

3.2.1.3 Additional tasking - Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Product Generation Executable (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are ${PGSHOME}/database/common/TD/leapsec.dat and ${PGSHOME}/database/common/CSC/utcpole.dat. The update of these files is accomplished by executing leapsec_update.sh and utcpole_update.sh in the /tools/admin/exec directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting.

3.2.2 Shutdown

Shutdown means that the system is being removed from a fully useable and operational state and possibly, power to the system will be terminated. The types of shutdown would vary depending upon circumstances (i.e. shutdown to single user mode; shutdown to power off; etc.)

3.2.2.1 Normal - By Subsystem

The Normal System Shutdown process is performed at the discretion of the SA usually for a scheduled repair. The system shutdown is **normally performed in reverse order of the system startup.**

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the OPR/SA has been properly trained to shutdown all aspects of the system.

This section explains how to perform a normal system shutdown by subsystem**.**

3.2.2.1.1 Shutdown a Machine

The OPR must be logged in as root to perform a shutdown. To begin a normal system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **wall** and press **Return**. Use **wall -a** on Sun machines to cross NFS mounts.

4 Type **This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.** then press **Return.** Press **Control** and **D** keys **simultaneously**. Include your name and closest telephone number.

5 Wait at least five minutes.

6 Type **shutdown -g600 -i0 -y** UNIX prompt and press **Return**. (600 = Number of Seconds)

7 When the system is at the prompt it is safe to ***Power off*** all peripherals first, and then the CPU.

The servers should be shutdown in the reverse order of the startup:

1 Determine which machines are dependent on a server first:

- Once each system has stopped without error, power off peripherals
- Proceed to the following machine
- Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine for each machine

2 The **NIS server** must be the **last system** to be shutdown.

Table 3.2-4 presents the **QUICK STEP** procedure required to perform a normal system shutdown.

Table 3.2-4. Normal System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine subsystems and server dependencies**
2	(No entry)	**Login to the server as root**
3	**wall**	**Press Return**
4	**This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.**	**Press Control and D keys simultaneously**
5	(No entry)	**Wait at least five minutes**
6	**shutdown -g600 -i0 -y** **- OR -** **shutdown now -i0 -y**	**Press Return**
7	(No entry)	**Power off all peripherals and the CPU.**
8	(No entry)	**Repeat steps 2 through 7 above for all servers Table 3.2.2**

3.2.2.2 Emergency - By Subsystem

The Emergency System Shutdown process begins after it is determined that the system may fail during emergency situations (i.e., storms, power outages) by the System Administrator (SA). The Emergency System Shutdown is done in sequential order by subsystem. This shutdown sequence is predetermined by the SA.

The NIS server must be the last system to shutdown.

Detailed procedures for tasks performed by the OPR/SA are provided in the sections that follow.

This section explains how to perform an emergency system shutdown by subsystem. The OPR must be logged in as root to perform a shutdown. To begin an emergency system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **sync** at the UNIX prompt and hit **Return**.

- Sync executes the sync system primitive. If the system is to be stopped, sync must be called to insure file system integrity. It will flush all previously unwritten system buffers out to disk, thus assuring that all file modifications up to that point will be saved.

4 Type **sync** again at the UNIX prompt and hit **Return**.

5 Type **halt** at the UNIX prompt and hit **Return**.

6 Once the halt has completed, turn the power switch on all the peripherals and the CPU off.

The servers should be shutdown in the following order:

1 Shutdown all client workstations.

2 ***Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine*** *for* ***<u>each</u>*** *machine*

3 The **NIS server** must be the **last system** to shutdown.

In case of ***EXTREME emergency*** where time does not allow you to execute the above procedures, execute the following procedure steps for ***Sun machines ONLY.***

1 Login to the server as root.

2 Enter root password.

3 Hit the L1 or Stop key and the a key simultaneously.

4 Once returned to an **ok** or > prompt, turn the power switches on the CPU and all peripherals to off.

NOTE: The use of L1a does not ensure file system integrity. There is a very high risk of losing data when using this process.

Table 3.2-5 presents the **QUICK STEP** procedures required to perform an Emergency System Shutdown.

Table 3.2-5. Emergency System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine subsystems and server dependencies**
2	(No entry)	**Login to server as root**
3	(No entry)	**Type sync at prompt and press enter**
4	(No entry)	**Type sync at prompt and press enter**
5	(No entry)	**Type halt at prompt and press enter**
6	(No entry)	**Turn power switches on CPU and all peripherals to off.**
7	(No entry)	**Repeat steps 2 through 5 above for all servers**

3.2.2.3 Server - By Server Software

The System Shutdown by Server Software process is performed by the OPR. The system shutdown is normally performed in reverse order of the system startup.

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to shutdown all aspects of the system.

Table 3.2-6 presents the QUICK STEP procedure required to perform a normal system shutdown.

Table 3.2-6. Server System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine software dependencies**
2	(No entry)	**shutdown dependent server(s)**
3	(No entry)	**shutdown independent server(s)**

3.3 System Backup and Restore

Performing regular and comprehensive system backups is one of the most important requirements of ECS operations. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore all of the data from the backup tapes. Accordingly, ECS includes a software product, *Legato Networker*, which is set up to perform backups automatically on a regular periodic basis. The backups copy critical data to digital linear tape, and Networker can be configured to make *clones* or copies of some or all of these data, so that it is possible to store the data (e.g., full system backups) in offsite secure storage.

System Backup is the process of copying the information from the machine, either the entire or partial system, for safe keeping for a specific time period. Restore is the process of returning the data to the machine to allow operation to continue from a specific point in time. The operator must be in the admin list to configure and use Networker. This is not root privilege, although **root** on the Networker server has admin privileges.

An ***incremental backup*** copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users.

Incremental backups are performed automatically according to the schedule set up in the Networker Schedules windows. Incremental backups can also be requested at unscheduled times by completing the **Incremental Backup Request Form** and submitting it to the OPS Supervisor.

A ***full system backup*** is a snapshot of the data on the entire system as of a particular date. The data are stored on tapes that are used to recreate the system in the event of a total system failure. Networker runs the full system backup on a regular schedule, usually weekly.

Refer to local procedures for software backup requirements including offsite backups. The procedural information in this document includes information concerning reconfiguration of the Networker setup for backups, with specific provisions for offsite storage of full backup data. Section 3.3.1 concerns incremental backups. Section 3.3.2 includes specific reference to offsite storage of full backup data. Section 3.3.3 addresses reconfiguration of Networker setup to enable the removal of backup tapes for offsite storage.

3.3.1 Incremental Backup

Non-scheduled incremental backups can be requested at any time by submitting a request through **REMEDY** for ***Incremental Backup*** to the **OPS supervisor**. The supervisor schedules the request with the operator who performs the incremental backup. Afterwards, the operator notifies the requester and supervisor that the incremental backup is complete.

The **Activity Checklist** in Table 3.3-1 provides an overview of the incremental backup processes. ***Note***: This is for manual backup outside Networker's automatic backup schedule.

Table 3.3-1. Incremental Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for **Incremental** Backup to OPS Supervisor.	(I) 3.3.1	
2	OPS Super	Schedule Incremental Backup with operator.	(I) 3.3.1	
3	Operator	Perform Incremental Backup.	(P) 3.3.1	
4	Operator	Notify Requester and OPS Super when Incremental Backup is Complete.	(I) 3.3.1	

Detailed procedures for tasks performed by the operator are provided in the sections that follow.

The procedures assume that the requester's request for an incremental backup has already been approved by DAAC Management. Incremental backups can be requested at any time by submitting a request for ***Incremental Backup*** to the **OPS supervisor**. In order to perform the procedure, the operator must have obtained the following information from the requester:

a. **Name of machine(s) to be backed up**

b. **Files/directories to be backed up (optional)**

Table 3.3-2 presents the steps required to perform a non-scheduled incremental backup. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

Note: If you run out of tapes at any time during this procedure, execute procedure 3.3.6.1 Labeling Tapes and then return to this procedure.

1 Log into the machine to be backed up by typing: **ssh** ***BackedUpSystemName***, then press the **Return/Enter** key.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press the **Return/Enter** key.
- Or press **Return** twice to get the Password prompt.

3 Enter ***YourPassword***, then press the **Return/Enter** key.
- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press the **Return/Enter** key.
- A password prompt is displayed.

5 Enter the ***RootPassword***, then press the **Return/Enter** key.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the NetWorker Administrative program by entering: **nwadmin &**, then press the **Return/Enter** key.
- A window opens for the Networker Administrative program.
- You are now able to perform an incremental backup.

7 Click **Clients**.
- Click **Client Setup**.
- Click Host Being Backed Up.
- Highlight the group to be Backed Up.

8 Go to the **Customize** menu, select **Schedules**.
- The **Schedules** window opens.

9 Look at the button for today. If there is an **i** next to the date on this button, go to step 12.
- The **i** stands for incremental.
- The **f** stands for full.
- Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.

10 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.

11 Click the **Apply** button.

12 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

13 Click the **Group Control** button.
- The **Group Control** window opens.

14 Click the **Start** button.
- A **Notice** window opens.

15 Click the **OK** button.
- The **Notice** window closes.
- The regularly scheduled backup will still run (even though we are now doing a backup).

16 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.
- Status updates appear in the **nwadmin** window.

- When the backup is complete, a **Finished** message will appear.

17 If the button for today in step 9 had an **i** on it, go to step 21.

18 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

19 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.

20 Click the **Apply** button.

21 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

22 Select **Exit** from the **File** menu to quit the Networker Administrative program.

- The **nwadmin** window closes.

23 At the UNIX prompt for the **machine to be backed up***,* type **exit** then press the **Return/Enter** key.

- **Root** is logged out.

24 Type **exit** again, then press the **Return/Enter** key.

- You are logged out and disconnected from the **machine to be backed up**.

Table 3.3-2. Perform Incremental Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** *BackedUpSystemName*	enter text; press **Return/Enter**
2	*YourPassphrase* **or-** (No entry)	enter text; press **Return/Enter** -or- (No action)
3	*YourPassword*	enter text; press **Return/Enter**
4	**su**	enter text; press **Return/Enter**
5	*RootPassword*	enter text; press **Return/Enter**
6	**nwadmin &**	enter text; press **Return/Enter**
7	Click **Clients** Click **Client Setup** Click Host Being Backed Up - Highlight the Group to be Backed Up	**click** options
8	Menu path **Customize** → **Schedules**	**click** option
9	Observe button for today; if **i**, go to Step 12	**read text**
10	Hold button for today to obtain menu; menu path **Overrides** → **Incremental**	**click** option
11	Activate **Apply** button	**single-click**
12	Close **Schedules** window	**click select**
13	Activate **Group Control** button	**single-click**
14	Activate **Start** button	**single-click**
15	Activate **OK** button	**single-click**
16	Close **Group Control** window	**click select**
17	(No entry)	**if there was an i on today's button in step 8, go to step 17.**
18	Menu path **Customize** → **Schedules**	**click** option
19	Hold button for today to obtain menu; menu path **Overrides** → **Full**	**click** option
20	Activate **Apply** button	**single-click**
21	Close **Schedules** window	**click select**
22	Menu path **File** → **Exit**	**click** option
23	**exit**	**press Return**
24	**exit**	**press Return**

3.3.2 Full Backup

Non-scheduled full backups can be requested at any time by submitting a request for ***Full Backup*** to the OPS supervisor. The supervisor schedules the request with the operator who performs the full backup. Afterwards, the operator notifies the requester and supervisor that the full backup is complete. In preparation for offsite storage, it is also necessary to copy the file index to a tape for storage offsite with the system backups.

The **Activity Checklist** in Table 3.3-3 provides an overview of the full backup processes.

Table 3.3-3. Full Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for **Full** Backup to OPS Supervisor.	(I) 3.3.2	
2	OPS Super	Schedule Full Backup with operator	(I) 3.3.2	
3	Operator	Perform Full Backup.	(P) 3.3.2	
4	Operator	Notify Requester and OPS Super when Full Backup is Complete.	(I) 3.3.2	

Detailed procedures for tasks performed by the operator are provided in the sections that follow.

The procedures assume that the requester's application for a full backup has already been approved by DAAC Management. In order to perform the procedure, the operator must have obtained the following information from the requester:

a. **Name of machine to be backed up**

b. **Files/directories to be backed up** (optional)

Table 3.3-4 presents the steps required to perform a full backup for the requester. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

Note: If you run out of tapes at any time during this procedure, execute procedure 3.3.6.1 Labeling Tapes and then return to this procedure.

1 To log into the machine to be backed up, type **ssh** ***<hostname>*** and then press the **Return/Enter** key.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press the **Return/Enter** key.
- Or press the **Return/Enter** key twice to get to Password prompt.

3 Enter ***YourPassword***, then press the **Return/Enter** key**.**
- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press the **Return/Enter** key.
- A password prompt is displayed.

5 Enter the ***RootPassword***, then press the **Return/Enter** key.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the Networker Backup program by entering **nwbackup &**, then press the **Return/Enter** key.
- A **Networker Backup** window opens.
- You are now able to perform a full backup.

7 Click **Clients**.

- Click Client Setup
- Click Host Being Backed Up
- Highlight the group to be Backed Up

8 If no list of **files/directories to be backed up** was provided, i.e. the whole machine is to be backed up, then type / in the **Selection** field; otherwise, go to Step 10.

- The character / is displayed in the **Selection** field.

9 Click the **Mark** button and then go to Step 12.

- A check mark next to / indicates that it is designated for backup.

10 If names of **file(s)/directory(ies) to be backed up** were provided, then click to select the **file(s)/directory(ies) to be backed up** in the directory display.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on a directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.

11 Click the **Mark** button.

- A check mark next to each selected file indicates that it is designated for backup.

12 Click the **Start** button.

- A **Backup Options** window opens.

13 Click the **OK** button.

- The **Backup Options** window closes.
- The **Backup Status** window opens providing updates on the backup's progress.

14 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.

- The **Backup Status** window closes.
- The backup is complete.

15 Select **Exit** from the **File** menu to quit the Networker Backup program.

- The **Networker Backup** window closes.

16 To copy the file index to tape for offsite storage, type **cp** ***<index_filename> <tape distination>***.

17 Remove the cloned system full backup tapes from the STK jukebox for transport to secure offsite storage.

18 Replace the removed system backup tapes with a set of backup tapes rotated in from secure offsite storage.

19 At the UNIX prompt*,* type **exit** and then press the **Return/Enter** key.

- **Root** is logged out.

20 Type **exit** again, and then press **Return/Enter** key.

- You are logged out and disconnected from the **machine to be backed up**.

Table 3.3-4. Perform Full Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh <*hostname*>**	enter text; press **Return/Enter**
2	*YourPassphrase* **or-** (No entry)	enter text; press **Return/Enter** -or- (No action)
3	*YourPassword*	enter text; press **Return/Enter**
4	**su**	enter text; press **Return/Enter**
5	*RootPassword*	enter text; press **Return/Enter**
6	**nwbackup &**	enter text; press **Return/Enter**
7	Click Client Click **Client Setup** Click Host Being Backed Up - Highlight the Group to be Backed Up	**click** options
8	If the whole machine is to be backed up, click in the **Selection** field and type **/**; otherwise, go to Step 10	**click**; enter text
9	Activate the **Mark** button	**single-click**
10	If only certain files/directories are to be backed up, select the file(s)/directory(ies) in the directory display.	**click**
11	Activate the **Mark** button	**single-click**
12	Activate the **Start** button	**single-click**
13	Activate the **OK** button in the **Backup Options** window	**single-click**
14	Activate the **Cancel** button in the **Backup Status** window	**single-click**
15	Menu path **File → Exit**	**click** option
16	To copy the file index to tape for offsite storage, **cp <*index_filename*><*tape destination*>**	enter text; press **Return/Enter**
17	Remove the cloned system full backup tapes from jukebox for transport to secure offsite storage	transport backup tapes and tape with index to offsite storage
18	Replace the removed system backup tapes with a set rotated in from secure offsite storage	insert tapes
19	**exit**	enter text; press **Return/Enter**
20	**exit**	enter text; press **Return/Enter**

3.3.3 Configuring Networker Setup for Backup Clones for Offsite Storage

Detailed information on configuring Networker may be found in the *Legato Networker Administrator's Guide, UNIX Version*. During installation at the sites, Networker is configured to schedule and perform automatic incremental and full backups. Therefore, much of the initial setup is complete, including licensing, designation of users who have administrative privileges, specification of *clients* (computers that contain data to be backed up) and their *save sets* (increments of data to be backed up), and identification of storage devices. If Networker is not configured to create any *clones* (duplicate copies of save sets) that can be removed from the storage device and stored at an offsite location, it will be necessary to change the *pools* (collections of backup tape volumes in the storage device) to implement offsite storage. Specifically, it will be appropriate to specify separate pools for full backups and incremental backups, and for clones of the associated full backup save sets that can be stored off site.

The purpose of off-site storage of backup data is to enable restoration of the system in the unlikely circumstance of a catastrophic event that causes loss of system software. In the face of such an event, in order to return to operational status, once the system hardware and infrastructure have been determined sound or returned to sound condition, it will be necessary to reload the operating system and restore the system from the backup data. This will require not only the offsite backup data, but also access to media containing the operating system software, *Legato* Networker software, and indexes to the backup data. Accordingly, it is necessary to secure in offsite storage the operating system software media, Networker software media, and media containing the indexes for backup data, as well as the backup data themselves.

To set up the system for off-site backups, it is necessary to create a label template (used by Networker to create internal labels for tapes) and create a clone pool for the tapes to be used in cloning the full backup for offsite storage. When creating any volume pool in Networker, it is necessary to specify the type of data to include on the volumes in the pool; one of the preconfigured selections provided by Networker is Backup Clone, and this may be used for the type of data to include on volumes in the clone pool.

The **Activity Checklist** in Table 3.3-5 provides an overview of the process to configure Networker to clone full backups, copy the necessary indexes, and ensure offsite storage of the necessary data.

Table 3.3-5. Configure Networker to Enable Offsite Storage - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Operator	Set up Label Template.	(P) 3.3.3	
2	Operator	Set up Clone Pool.	(P) 3.3.3	

Table 3.3-6 presents the steps required to configure Networker for offsite storage (i.e., to set up for cloning full backups). If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 Start the log-in to the Tape Backup server by typing **/tools/bin/ssh *hostname*** (e.g., **g0mss07**, **e0mss04**, **l0mss05**, or **n0mss05**) and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** ("y" alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- This procedure assumes you are set up as an administrative user. If you are not, and are not **root**, you will not be able to change the configuration.

5 At the ***<user@remotehost>*'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

- This procedure assumes you are set up as an administrative user. If you are not, and are not **root**, you will not be able to change the configuration.
- You are authenticated and returned to the UNIX prompt.

6 Execute the Networker Admin program by entering **nwadmin &** and then press the **Return/Enter** key.

- The **nwadmin** window is displayed.

7 To begin creation of a label template, follow menu path **Customize→Label Templates . . . .**

- The **Label Templates** window is displayed.

8 Click on the **Create** button.

- The data fields are cleared and the cursor is displayed in the **Name:** field.

9 Type **Full Clone** and then press the **Tab** key.

- The typed entry is displayed in the **Name:** field and the cursor is displayed in the **Fields:** field.

10 Type **<*NetworkerHostName*>.ecs.nasa.gov** and then press the **Tab** key.

- For **<*NetworkerHostName*>**, use the Tape Backup server for Networker at the local site (e.g., **g0mss07**, **e0mss04**, **l0mss05**, or **n0mss05**).
- The typed entry is displayed in the **Fields:** field and in the list window immediately below the field.

11 Replace the entry in the **Fields:** field with **Full** (e.g., use the mouse to highlight the entry in the field and then type **Full** over it, or click at the end of the field and use the backspace key to delete the entry before typing **Full**) and then press the **Tab** key.

- The typed entry is displayed in the **Fields:** field and in the list window immediately below the field.

12 Replace the entry in the **Fields:** field with **001-999** (e.g., use the mouse to highlight the entry in the field and then type **001-999** over it, or click at the end of the field and use the backspace key to delete the entry before typing **001-999**) and then press the **Tab** key.

- The typed entry is displayed in the **Fields:** field and is added to the list window immediately below the field.

13 In the **Separator:** field, click on the selection button next to the symbol to be used as a separator between components of the labels (choices are "**.**", "**_**", "**:**", and "**-**"; use the "**.**").

- The button changes color to indicate the selection.

14 Click on the **Apply** button.

- The **Next:** field displays **<*NetworkerHostName*>.ecs.nasa.gov.Full.001** to indicate the next label that will be applied.

15 Follow menu path **File→Exit**.

- The **Label Templates** window is closed.

16 To begin creation of the Full Backup clone pool, on the Networker main window, follow menu path **Media→Pools . . . .**

- The **Pools** window is displayed.

17 Click on the **Create** button.

- The cursor is displayed in the **Name:** field.

18 Type **Full Clone** and then press the **Tab** key.

- The typed entry is displayed in the **Name:** field.

19 In the **Enabled:** field, make sure that the selection button for **Yes** indicates selection (click on the button if necessary).

- The selection button color indicates selection.

20 Click on the pull-down arrow at the right of the **Pool Type:** field and, holding down the right mouse button, drag to select **Backup Clone**.

- The selection is displayed in the **Pool Type:** field.

21 Click on the pull-down arrow at the right of the **Label Template:** field and, holding down the right mouse button, drag to select **Full Clone**.

- The selection is displayed in the **Label Template:** field.

22 In the **Store Index Entries:** field (use the scroll bar on the right side of the window to scroll down if necessary), click on the selection button for **Yes**.

- The button color changes to indicate selection.

23 Click on the **Apply** button.

- **Full Clone** is displayed in the **Pools:** list.

24 In the **Pools:** list, click on **Full**.

- **Full** is highlighted and data for the **Full** pool are displayed in the appropriate data fields.

25 To ensure that the **Full** pool can be used for full backups, in the **Enabled:** field, make sure that the selection button for **Yes** indicates selection (click on the button if necessary).

- The selection button color indicates selection.

26 Follow menu path **File→Exit** (in the **Pools:** window).

- The **Pools:** window is closed.

27 Follow menu path **File→Exit** (in the **nwadmin** window).

- The **nwadmin** window is closed.

Table 3.3-6. Configure Networker to Enable Offsite Storage

Step	What to Enter or Select	Action to Take
1	Access the UNIX command shell	
2	**setenv DISPLAY *clientname*:0.0**	enter text; press **Return/Enter**
3	**/tools/bin/ssh *hostname***	enter text; press **Return/Enter**
4	***Passphrase* or-** (No entry)	enter text; press **Return/Enter** -or- (No action)
5	***Password***	enter text; press **Return/Enter**
6	**nwadmin &**	enter text; press **Return/Enter**
7	Menu path **Customize→Label Templates . . .**	**click** option
8	Activate the **Create** button	**single-click**
9	Type **Full Clone** in the **Name:** field and then **Tab** to the **Fields:** field	enter text; press **Tab**
10	Type **<*NetworkerHostName*>.ecs.nasa.gov** in the **Fields:** field and then **Tab** to display the entry in the list window	enter text; press **Tab**
11	Enter **Full** in the **Fields:** field and then **Tab** to display the entry in the list window	enter text; press **Tab**
12	Enter **001-999** in the **Fields:** field and then **Tab** to display the entry in the list window	enter text; press **Tab**
13	In the **Separator:** field, select **.** as the separator to be used between components of the labels	**click** select
14	Activate the **Apply** button	**single-click**
15	Menu path **File →Exit**	**click** option
16	Menu path **Media →Pools . . .**	**click** option
17	Activate the **Create** button	**single-click**
18	Type **Full Clone** in the **Name:** field and then **Tab** to the **Enabled:** field	enter text; press **Tab**
19	In the **Enabled:** field, ensure that the selection button for **Yes** is selected	**single-click** (if necessary)
20	Activate **Pool Type:** pull-down arrow and select **Backup Clone**	**click** option
21	Activate **Label Template:** pull-down arrow and select **Full Clone**	**click** option
22	In the **Store Index Entries:** field, select **Yes**	**single-click**
23	Activate the **Apply** button	**single-click**
24	In the **Pools:** list, highlight **Full**	**single-click**
25	In the **Enabled:** field, ensure that the selection button for **Yes** is selected	**single-click** (if necessary)
26	Menu path **File →Exit** (for the **Pools:** window)	**click** option
27	Menu path **File →Exit** (for the **nwadmin** window)	**click** option

3.3.4 File Restore

SINGLE OR MULTIPLE FILES RESTORE

From time to time, individual files or groups of files (but not all files) will have to be restored from an Incremental or Full backup tape(s) due to Operator error or system failure. This can be accomplished using the following file restoration procedure.

The File Restore process begins when the requester submits a request to the Operator. The Operator restores the file(s) and notifies the requester when complete.

The **Activity Checklist** in Table 3.3-7 provides an overview of the file restore process.

Table 3.3-7. File Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for File Restore to Operator	(I) 3.3.4	
2	Operator	Restore file(s).	(P) 3.3.4	
3	Operator	Inform Requester of completion.	(I) 3.3.4	
4	Operator	Complete System Restore/Partition Restore	(P) 3.3.4	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

The procedures assume that the requester's application for a file restore has already been approved by the Ops Supervisor. In order to perform the procedure, the Operator must have obtained the following information from the requester:

a. **Name of machine to be restored**

b. **Name of file(s) to be restored**

c. **Date from which to restore**

d. **User ID of the owner of the file(s) to be restored**

e. **Choice of action to take when conflicts occur. Choices are:**

- **Rename current file**
- **Keep current file**
- **Write over current file with recovered file**

Table 3.3-8 presents the steps required to restore a file. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the following detailed procedure:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY** ***clientname*****:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 To start the log-in to the machine to be restored, type **/tools/bin/ssh <*hostname*>** and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** (“**y**” alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- Or press the **Return/Enter** key twice to get to the Password prompt.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key**.**

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt.

NOTE: Before executing the Networker Recovery ensure, that you are in the **/data1/COTS/networker** directory.

6 Execute the **Networker Recovery** program by entering **nwrecover &**, and then press the **Return/Enter** key.

- A window opens for the Networker Recovery program.
- You are now able to perform the file restoration.

7 Click to select the **file(s)/directory(ies) to be restored** in the directory display.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.

8 Click the **Mark** button.

- A check mark next to each selected file indicates that it is designated to be restored.

9 Go to the **Change** menu, select **Browse Time**.

- The **Change Browse Time** window opens.

10 Select the **date from which to restore**.

- Networker will automatically go to that day's or a previous day's backup which contains the file.

11 Click the **Start** button.

- The **Conflict Resolution** window opens.

12 Answer **Do you want to be consulted for conflicts** by clicking the **yes** button.

13 Click the **OK** button.

- If prompted with a conflict, choices of action will be: **rename current file**, **keep current file**, or **write over current file with recovered file**. Select the requesters **choice of action to take when conflicts occur**.
- The **Recover Status** window opens providing information about the file restore.
- If all the required tapes are not in the drive, a notice will appear. Click the **OK** button in the notice window.
- If prompted for tapes, click **Cancel** in the **Recover Status** window and execute procedure 3.3.6.2 Indexing Tapes.

14 When a recovery complete message appears, click the **Cancel** button.

15 Go to the **File** menu, select **Exit**.

- The **Networker Recovery** program quits.

16 Type **exit**, then press the **Return/Enter** key.

- The **owner of the file(s) to be restored** is logged out.

17 Type **exit** again, then press the **Return/Enter** key.

- You are logged out and disconnected from the **machine to be restored.**

Table 3.3-8. Restore a File - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Access the UNIX command shell	
2	**setenv DISPLAY *clientname*:0.0**	enter text; press **Return/Enter**
3	**/tools/bin/ssh *hostname***	enter text; press **Return/Enter**
4	***Passphrase*** -or- (No entry)	enter text; press **Return/Enter** -or- press **Return/Enter** twice
5	***Password***	enter text; press **Return/Enter**
6	**nwrecover &**	enter text; press **Return/Enter**
7	Select the file(s)/directory(ies) to be restored	**click** select
8	Activate the **Mark** button	**single-click**
9	Menu path **Change →Browse Time**	**click** option
10	Select **date from which to restore**	**click** select
11	Activate the **Start** button	**single-click**
12	Select **yes** for **Do you want to be consulted for conflicts?**	**single-click**
13	Activate the **OK** button; address any conflicts	**single-click**
14	Upon completion of recovery, activate the **Cancel** button	**single-click**
15	Menu path **File → Exit**	**click** option
16	**exit**	enter text; press **Return/Enter**
17	**exit**	enter text; press **Return/Enter**

3.3.5 Complete System Restore

The Complete System Restore process begins when the requester has determined that a complete system restore is the only way to resolve the problem and has approval from the Operations Supervisor. Once notified of the request, the Operator performs restores of all partitions on the system. Afterwards, the Operator documents and logs all actions in the operator's log book and notifies the requester and Ops Supervisor that the system restore is complete.

The **Activity Checklist** in Table 3.3-9 provides an overview of the complete system restore process.

Table 3.3-9. Complete System Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Trouble Shoot and Determine that a Complete System Restore is necessary.	(I) 3.3.5	
2	Operator	Restore all Partitions on the System	(P) 3.3.5	
3	Operator	Document and Log in operator's log book, and Inform Requester and Ops Supervisor of completion.	(I) 3.3.5	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow. The procedures assume that the requester's application for a complete system restore has already been approved by Ops Supervisor. In order to perform the procedures, the Operator must have obtained the following information about the requester:

a. **Name of system to be restored**

b. **Date from which to restore**

A complete system restore involves restoring all partitions on that system.

Table 3.3-10 presents the steps required to restore a partition. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the following detailed procedure:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 To start the log-in to the host that requires restoration, type **/tools/bin/ssh <*hostname*>** and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** (“**y**” alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- Or press the **Return/Enter** key twice to get to the Password prompt.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** then press the **Return/Enter** key**.**

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

6 To execute the **Networker Administrative** program, enter **nwadmin &** and then press the **Return/Enter** key.

- A window opens for the Networker Administrative program.
- You are now able to perform restores of partitions.

7 Go to the **Save Set** menu, select **Recover . . . .**

- The **Save Set Recover** window opens.

8 Click on the pull-down arrow at the right side of the **Client** field and select the **Name of system to be restored** (referred to as **System** in the rest of this procedure).

- The **Save Set** listing updates. This is a listing of partitions on the **System**.
- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.

9 In the **Save Set** list, click on the name of the partition for the restoration.

- The name is highlighted and the **Instances** listing is updated.

10 Click on the appropriate **Instance**.

- An Instance is a particular Networker client backup. A listing of Instances is a report detailed with the Networker client backups that have occurred.
- Select an Instance based upon the Date from which to restore (referred to as Date in the rest of this procedure) and an appropriate level; the selection is highlighted.

NOTE: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backups occur at 02:00 each morning, then a system corrupted at noon on June 6th would require a restoration of the June 6th backup. If the Backups are full or incremental, perform the following actions: Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.

If the backups are of different numerical levels, follow these steps:

1) Select the most recent level **0/full backup** prior to or on the **Date** and perform a restore of the partition.

2) If a level **0/full backup** did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level **0** and prior to or on the **Date**.

3) Perform a restore of the partition.

4) Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

11 Click the **Recover** button.

- The Save Set Recover Status window opens.
- Clicking the Volumes button will show which tapes are required.

12 Click the **Options** button.

- The **Save Set Recover Options** window opens.

13 Set **Duplicate file resolution** to **Overwrite existing file** by clicking its radio button.

14 Make sure that the **Always prompt** checkbox is not checked.

15 Click the **OK** button.

- The Save Set Recover Options window closes.

16 Click the **Start** button in the **Save Set Recover Status** window.

- Status messages appear in the Status box.
- If prompted for tapes, click the Cancel button in the **Save Set Recover Status** window and follow steps **1-18** of procedure **3.3.6.2** Index tapes (or steps 1-19 of procedures **3.3.6.2** Index Tapes Quick Steps)
- A **recovery complete** message appears when recovery is complete.

17 Click the **Cancel** button after the **recovery complete** message appears.

- The **Save Set Recover Status** window closes.

18 If additional partition restores are required, repeat steps 10 - 17; otherwise go to step 19.

19 When all desired restorations are complete, select **Exit** from the **File** menu to quit the Networker Administrative program.

- The **nwadmin** window is closed.

20 At the UNIX prompt for the backup server*,* type **exit**, then press the **Return/Enter** key.

- The **owner of the file(s) to be restored** is logged out.

21 Type **exit** again, then press the **Return/Enter** key.

- You are logged out and disconnected from the **machine to be restored.**

Table 3.3-10. Restore a Partition - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Access the UNIX command shell	
2	**setenv DISPLAY *clientname*:0.0**	enter text; press **Return/Enter**
3	**/tools/bin/ssh *hostname***	enter text; press **Return/Enter**
4	***Passphrase*** -or- (No entry)	enter text; press **Return/Enter** -or- press **Return/Enter** twice
5	***Password***	enter text; press **Return/Enter**
6	**nwadmin &**	enter text; press **Return/Enter**
7	Menu path **Save Set** →**Recover . . .**	**click** option
8	Use pull-down arrow in **Client** field to select the **Name of the system to be restored**	**click** option
9	Select the **Save Set**	**single-click**
10	Select the **Instance**	**single-click**
11	Activate the **Recover** button	**single-click**
12	Activate the **Options** button	**single-click**
13	Use radio button to set **Duplicate file resolution** to **Overwrite existing file**	**single-click**
14	Ensure that the **Always prompt** checkbox is NOT checked	**single-click** (if necessary)
15	Activate the **OK** button	**single-click**
16	In the **Save Set Recover Status** window, activate the **Start** button	**single-click**
17	After recovery is complete, activate **Cancel** button	**single-click**
18	For any additional partitions to be restored, repeat steps 10 - 17	
19	Menu path **File** →**Exit**	**click** option
20	**exit**	enter text; press **Return/Enter**
21	**exit**	enter text; press **Return/Enter**

3.3.6 Tape Handling

The following procedures describe how to label tapes, index tapes, and clean tape drives. Each of these procedures contains detailed steps that explain how to complete the procedure properly. Each tape handling procedure is significant in maintaining a working backup system. DAAC scheduled backups depend on proper maintenance of tape media and tape drives. Listed are complete explanations of the procedures and their relevance to the Computer Operator position.

The **Activity Checklist** in Table 3.3-11 provides an overview of the tape handling process.

Table 3.3-11. Tape Handling - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Labeling Tapes	(I) 3.3.6.1	
2	Operator	Indexing Tapes	(P) 3.3.6.2	
3	Operator	Tape Drive Cleaning	(P) 3.3.6.3	

3.3.6.1 Labeling Tapes

The Tape Labeling process begins when the Operator is performing procedures 3.3.1 Incremental Backup or 3.3.2 Full Backup (or their associated Quick Steps) and runs out of tapes. The tape(s) must be installed in the jukebox and labeled. Networker uses tape labels for identification. The label that Networker creates is on the tape media itself, rather than a sticker on the outside of the tape cassette. An index is kept by Networker associating tape labels with particular backups/data. When you select files to be recovered using the Networker Recovery window or view saved sets on a backup volume using the Volume Management window in Networker, you are viewing this index. After labeling the required tape(s), the Operator resumes procedure 3.3.1 or 3.3.2.

Table 3.3-12. Labeling Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Install Required Tape(s) in Jukebox	(P) 3.3.6.1.1	
2	Operator	8mm, D3, or DLT Tapes Labeling Process	(P) 3.3.6.1.2	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

3.3.6.1.1 Install Required Tape(s) in Jukebox

The procedures assume that the Operator was previously executing procedure 3.3.1 or 3.3.2. In order to perform the procedures, the Operator must have obtained the following:

a. **Blank tape(s)**

All tapes are stored in the storage cabinet located in the control room. There are five tapes in each box, and every box of tapes has a unique number. To begin finding tapes for recycling to be labeled and installed in the Jukebox, the lowest numbers of a tape or a box of tapes should be used. Do not recycle any tape or box of tapes that the numbers are higher or current.

3.3.6.1.2 8mm, D3, or DLT Tapes Labeling Process

Table 3.3-13 presents the steps required to label tapes. The process for labeling Digital Linear Tapes (DLTs) differs from that for labeling 8mm tapes or D3 tapes only in the host reflected in the name (see Step 11 below). If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 To start the log-in to the Tape Backup server, type **/tools/bin/ssh *hostname*** (e.g., **g0mss07**, **e0mss04**, **l0mss05**, or **n0mss05**) and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** (“**y**” alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- Or press the **Return/Enter** key twice to get to the Password prompt.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

6 Log in as root by typing **su** and then press the **Return/Enter** key.

- A password prompt is displayed.

7 Enter the ***RootPassword***, then press **Return/Enter.**

- Remember that passwords are case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

8 To launch the **Networker Administrative** program GUI, enter **nwadmin &** and then press the **Return/Enter** key.

- The **Networker Administrative** program GUI is displayed.

9 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

- Remove all non-blank tapes from the cartridge or else they will be re-labeled and any data on the tapes will be lost.
- Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape. Do not enter any tape in Slot 11 for labeling.
- It is OK to leave empty slots.

10 Click the **Label** button from the menu bar.

- The **Jukebox Labeling** window opens.

11 In the **Starting with:** field, enter the tape label you wish to use for the first tape in the sequence and then press the **Tab** key.

- Tape labels are named by using the host name (e.g., **sprn1sgi**, or, for DLTs, **SPRDLT**), a dot or period, and a sequential number (e.g., **001**, **002**).
- By default, the system will prompt you with the next label in the sequence (e.g., **sprn1sgi.001**, or, for DLTs, **SPRDLT.001**).
- The cursor moves to the **First slot:** field.

12 In the **First slot:** field, enter **1** or the slot containing the first volume to be labeled and then press the **Tab** key.

- Slot 1 is at the top of the cartridge.
- The cursor moves to the **Last slot:** field.

13 In the **Last slot:** field, enter **10** or the slot containing the last volume to be labeled.

- Slot 10 is at the bottom of the cartridge (except for Slot 11, with the cleaning cartridge).

14 Click the **OK** button.

- A status message appears and updates.
- Labeling a full cartridge of tapes takes about 15 minutes.

15 When the status in the **Jukebox Labeling** window reads **finished**, click the **Cancel** button.

- The **Jukebox Labeling** window closes.

16 Go to the **File** menu and select **Exit**.

17 Put a sticker on the outside of each tape cassette.

- This is done in order for you to identify each tape.

Table 3.3-13. 8mm, D3, or DLT Tapes Labeling Process

Step	What to Enter or Select	Action to Take
1	Access the UNIX command shell	
2	**setenv DISPLAY *clientname*:0.0**	enter text; press **Return/Enter**
3	**/tools/bin/ssh *hostname***	enter text; press **Return/Enter**
4	***Passphrase*** -or- (No entry)	enter text; press **Return/Enter** -or- press **Return/Enter** twice
5	***Password***	enter text; press **Return/Enter**
6	Type **su**	enter text; press **Return/Enter**
7	***RootPassword***	enter text; press **Return/Enter**
8	**nwadmin &**	enter text; press **Return/Enter**
9	Place cartridge with blank tapes in jukebox	mount cartridge
10	Activate the **Label** button	**single-click**
11	Type ***<host>.nnn*** in the **Starting with:** field	enter text; press **Tab**
12	Type **1** (or first occupied slot) in the **First Slot** field	enter text; press **Tab**
13	Type **10** (or last occupied slot) in the **Last Slot** field	enter text; press **Return/Enter**
14	Activate the **OK** button.	**single-click**
15	When **finished**, activate the **Cancel** button	**single-click**
16	Menu path **File→Exit**	**click** option
17	Put a sticker on the outside of each tape cassette	mark tapes for identification

3.3.6.2 Indexing Tapes

The Indexing Tapes process begins when the Operator has finished performing procedures 3.3.6.1, (**Tape Labeling**). If the tape(s) is/are not ***indexed/inventoried,*** Networker will not be aware of it/them. After indexing the required tape(s), the Operator resumes procedure 3.3.1 or 3.3.2.

The **Activity Checklist** in Table 3.3-14 provides an overview of the indexing tapes process.

Table 3.3-14. Indexing Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Pull Required Tape(s) from Tape Storage.	(I) 3.3.5.2.1	
2	Operator	Index Tapes	(P) 3.3.5.2.2	

3.3.6.2.1 Pull Required Tape(s) from Tape Storage

In order to perform the procedure, the Operator must have obtained the following:

a. **The required tape(s)**.

This may necessitate retrieving tapes from secure offsite storage if other backups are unavailable.

3.3.6.2.2 Index Tapes

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

The procedures assume that the Operator has previously executed procedure 3.3.6.1, **Tape Labeling**.

Table 3.3-15 presents the steps required to index tapes. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 To start the log-in to the Tape Backup server, type **/tools/bin/ssh *hostname*** (e.g., **g0mss07**, **e0mss04**, **l0mss05**, or **n0mss05**) and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** (“**y**” alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- Or press the **Return/Enter** key twice to get to the Password prompt.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt.

6 To launch the **Networker Administrative** program GUI, enter **nwadmin &** and then press the **Return/Enter** key.

- The **Networker Administrative** program GUI is displayed.
- You are now able to index tapes.

7 If it is desired to see what tapes are currently available to **Networker**, click the **Mount** button.

- The **Jukebox Mounting** window is displayed.

8 If necessary, to dismiss the **Jukebox Mounting** window, click the **Cancel** button.

- The **Jukebox Mounting** window is closed.

9 Put the required tape(s) in the jukebox's cartridge and install the cartridge in the jukebox.

- For instructions, refer to the jukebox's documentation.

10 Go to the **Media** menu, select **Inventory**.

- The **Jukebox Inventory** window opens.

11 In the **First slot:** field, enter **1** or the slot containing the first volume to be indexed and then press the **Tab** key.

- Slot 1 is at the top of the cartridge.
- The cursor moves to the **Last slot:** field.
- It is OK to have empty slots or slots with tapes which have already been indexed.

12 In the **Last slot:** field, enter **10** or the slot containing the last volume to be indexed.

13 Click the **OK** button.

- A checking volume message appears and updates.
- Performing an inventory on a full cartridge takes twenty to thirty minutes.

14 When the status in the **Jukebox Inventory** window says **finished**, click the **Cancel** button.

- The **Jukebox Inventory** window closes.

15 Click the **Mount** button to verify that the indexing worked.

- The **Jukebox Mounting** window opens.
- The required tape(s) should be shown. If not, repeat from step 10.

16 Click the **Cancel** button.

- The **Jukebox Mounting** window closes.

17 Go to the **File** menu, select **Exit**.

18 At the UNIX prompt for the ***backup server,*** type **exit**, then press **Return**.

19 Type **exit** again, then press **Return**.

Table 3.3-15. Index Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Access the UNIX command shell	
2	**setenv DISPLAY *clientname*:0.0**	enter text; press **Return/Enter**
3	**/tools/bin/ssh *hostname***	enter text; press **Return/Enter**
4	***Passphrase*** -or- (No entry)	enter text; press **Return/Enter** -or- press **Return/Enter** twice
5	***Password***	enter text; press **Return/Enter**
6	**nwadmin**	enter text; press **Return/Enter**
7	If desired, activate the **Mount** button	**single-click**
8	If necessary to dismiss **Jukebox Mounting** window, activate the **Cancel** button	**single-click**
9	Place cartridge, with tapes to be indexed, in jukebox	mount cartridge
10	Menu path **Media →Inventory**	**click** option
11	Type **1** (or first occupied slot) in the **First Slot** field	enter text; press **Tab**
12	Type **10** (or last occupied slot) in the **Last Slot** field	enter text
13	Activate the **OK** button	**single-click**
14	When **finished**, activate the **Cancel** button	**single-click**
15	Activate the **Mount** button	**single-click**
16	Activate the **Cancel** button	**single-click**
17	Menu path **File →Exit**	**click** option
18	**exit**	enter text; press **Return/Enter**
19	**exit**	enter text; press **Return/Enter**

3.3.6.3 Tape Cleaning Process

The system will at times prompt for drive(s) cleaning, typically during non-processing periods. However, during the course of the tape backup process period, the drive(s) may send a request for cleaning. Manual cleaning should be performed each time tapes are installed in the jukebox. Maintaining clean drives can help prevent backup interruption that may occur due to unclean tape drive heads. If the system is prompted for drive(s) cleaning, follow the detailed steps below:

1 Access the UNIX command shell.

- The command shell prompt is displayed.

2 Type **setenv DISPLAY *clientname*:0.0** and then press the **Return/Enter** key.

- Use either the terminal/workstation IP address or the machine name for the ***clientname***.

3 To start the log-in to the Tape Backup server, type **/tools/bin/ssh *hostname*** (e.g., **g0mss07**, **e0mss04**, **l0mss05**, or **n0mss05**) and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** (“**y**” alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 4.
- If you have not previously set up a secure shell passphrase, go to Step 5.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 6.

- Or press the **Return/Enter** key twice to get to the Password prompt.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt.

6 To launch the **Networker Administrative** program GUI, enter **nwadmin &** and then press the **Return/Enter** key.

- A **Networker** administrative program GUI is displayed.

7 Highlight the desirable drive(s) that the system has prompted for cleaning.

8 Click dismount from the menu bar and wait a few minutes for the drive to be dismounted completely.

9 Repeat Steps 6 - 8 on the second drive until the both are dismounted.

To open the Exabyte door turn the key in the door counter clockwise. The last tape at the bottom of the cartridge is the cleaning tape. Remove it from the slot field and insert it gently into each drive below. Wait until the tape has been ejected and the flashing lights on the drive are off before removing the tape from the drive. Insure that the cleaning tape is still usable before each use. Cleaning tapes will expire after several uses. After each use mark the appropriate box on the surface of the tape to maintain a list of usage. Insert the cleaning tape back into the last slot and lock the Exabyte door.

3.4 User Administration

Note: User Administration procedures will be implemented through command-line and/or script entries.

3.4.1 Adding a User

The Adding a User process begins when the requester fills out a "User Registration Request Form" (located in Appendix A), and submits it to the site supervisor. The "User Registration Request Form" includes information regarding the user (User’s Name, Group, Organization, etc.), as well as the user's explanation of why an account on the system is needed. The requester's supervisor reviews the request, and if it is determined that it is appropriate for the requester to have a UNIX account, forwards the request to the Operations Supervisor (OPS Super). The OPS Super reviews the request and forwards it to the System Administrator (SA). The SA verifies that all required information is contained on the form. If it is, the SA implements the request. (Incomplete forms are returned to the requester’s supervisor for additional information.) After the user is registered, the SA provides the user with a password to use for logging onto their accounts. The SA also sends an e-mail message to the user's supervisor and the OPS Super, informing them that the user's accounts were created.

Table 3.4-1, the **Activity Checklist** table that follows, provides an overview of the adding a user process.

Table 3.4-1. Adding a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete User Registration Form and forward to the Supervisor.	(I) 3.4.1	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.1	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.1	
4	SA	Review User Registration Form for Completeness.	(I) 3.4.1	
5	SA	Add User.	(P) 3.4.1	
6	SA	Phone/e-mail User with Password. Notify Supervisor and OPS Super that user was added.	(I) 3.4.1	

Depending upon the script utilized, in order to add a new user the SA should obtain information such as the following about the requester:

a. **Real name of the new user**

b. **User name of the new user**

c. **Office number of the new user**

d. **Office phone number of the new user**

e. **Home phone number of the new user**

f. **Organization**

g. **Group affiliation(s)**

h. **Role(s) of the new user**

The SA creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser,* to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

3.4.2 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to the user's supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Supervisor reviews the request and forwards it to the SA, who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

The Activity Checklist table that follows provides an overview of the deleting a user account process.

Table 3.4-2. Deleting a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Determine that No Useful Files Remain in the User's Home Directory and Submit Request to user's Supervisor.	(I) 3.4.2	
2	OPS Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.2	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.2	
4	SA	Delete User.	(P) 3.4.2	
5	SA	Notify Requester, Supervisor and OPS Super that user was deleted.	(I) 3.4.2	

The process assumes that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **UNIX login of the user to be deleted**

b. **Role(s) of the user to be deleted**

The SA deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown,* to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion, deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

3.4.3 Changing a User Account Configuration

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Supervisor detailing what to change about the account configuration and the reason for the change. The OPS Supervisor reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

Table 3.4-3, the Activity Checklist table that follows, provides an overview of the changing a user account configuration process.

Table 3.4-3. Change a User Account Configuration - Activity Checklist

Order	Role	Task	Section	Complete?

1	Requester	Submit Request to OPS Supervisor.	(I) 3.4.3	
2	OPS Super	Review and Forward to SA.	(I) 3.4.3	
3	SA	Change User Account Configuration.	(P) 3.4.3	
4	SA	Inform Requester and Supervisor of completion.	(I) 3.4.3	

The process assumes that the requester’s application for changing a user account configuration has already been approved by the OPS Supervisor. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **What to change and new settings.**

Can be any of:

New Real User Name

New Login ID

New Office Number

New Office Phone Number

New Home Phone Number

New UNIX Group

New Login Shell

b. **Current UNIX Login of the User**

The SA changes the appropriate configuration items manually in the users home directory.

3.4.4 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to the supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and OPS Super.

Table 3.4.4, the Activity Checklist table that follows, provides an overview of the changing user access privileges process.

Table 3.4-4. Changing User Access Privileges - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.4	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.4	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.4	
4	SA	Change User Access Privileges.	(P) 3.4.4	

5	SA	Inform Requester, Supervisor and DAAC Mgr of completion.	(I) 3.4.4	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing user access privileges has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **Role(s) to which the user is to be added**

b. **Role(s) from which the user is to be removed**

c. **UNIX login of the user**

To change user access privileges for the requester, execute the procedure steps that follow:

3.4.5 Changing a User Password

The Changing a User Password process begins when the requester submits a request to the SA. The SA verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Table 3.4-5, the **Activity Checklist** table that follows, provides an overview of the changing a user password process.

Table 3.4-5. Changing a User Password - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to SA.	(I) 3.4.5	
2	SA	Verify that the Requester is Who S/he Claims to Be.	(I) 3.4.5	
3	SA	Change Password.	(P) 3.4.5	
4	SA	Inform Requester of completion.	(I) 3.4.5	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New password for the user**

To change a user password for the requester, execute the procedure steps that follow:

3.4.6 Checking a File/Directory Access Privilege Status

The Checking a File/Directory Access Privilege Status process begins when the requester submits a request to the SA. The SA checks the file/directory access privilege status and reports the status back to the requester.

Table 3.4-6, the **Activity Checklist** that follows provides an overview of the checking a file/directory access privilege status process.

Table 3.4-6. Checking a File/Directory Access Privilege Status - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit a Request to the SA.	(I) 3.4.6	
2	SA	Check a File/Directory Access Privilege Status.	(P) 3.4.6	
3	SA	Inform Requester of completion and Report the File/Directory Access Privilege Status.	(I) 3.4.6	

Detailed procedures for tasks performed by the SA are provided in the sections that follow. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which privilege status is needed**

Table 3.4-12 contains a table which presents the steps required to check a file/directory access privilege status in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To check a file/directory access privilege status for the requester, execute the procedure steps that follow:

1 At a UNIX prompt, type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe then type **cd /home** and press **Return**.

2 Type **ls -la | grep *FileOrDirectoryName***, press **Return**.
This command will return information like this:

```
drwxr-xr-x   19 jdoe user      4096 Jun 28 09:51 jdoe
-r-xr--r--    1   jdoe user       80    Jun 22 11:22 junk
```

What this output means, from left to right, is:

The file type and access permissions:

The *first character* indicates what type of file it is:

d means that the file is a directory.

- means that the file is an ordinary file.

l means that the file is a symbolic link.

The *next three characters* indicate the owner privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the owner (jdoe) of the file ***junk*** does not have *write* permissions, so a - appears rather than a w.

The *next three characters* indicate the group privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the group (user) of the directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the sixth character in the line.

The *next three characters* indicate the privileges that everyone else/other has, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** other in the case of the directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the ninth character in the line.

There are 19 links to the file/directory ***jdoe***.
The owner of the file/directory is jdoe.
The file/directory's group is user.
The file/directory is 4096 bytes large.
The last time the file/directory was modified is Jun 28 at 09:51.
The name of the file/directory is jdoe.

3 Create a report of the file/directory's access privilege status by using the information produced by step 2 and by filling out this template:

full path of the file/directory: ____________________________________

owner: ____

group: ____

owner/user privileges: _____ read _____ write _____ execute

group privileges: _____ read _____ write _____ execute

everyone else/other privileges: _____ read _____ write _____ execute

To check a file/directory access privilege status, execute the steps provided in table 3.4-7.

Table 3.4-7. Check a File/Directory Access Privilege Status - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**cd** ***Path***	**press Return**
2	**ls -la | grep** ***FileOrDirectoryName***	**press Return**
3	(No entry)	**generate a file/directory access privilege status report**

3.4.7 Changing a File/Directory Access Privilege

The Changing a File/Directory Access Privilege process begins when the requester submits a request to the supervisor to have file/directory access privileges changed. The supervisor approves/denies the request. When approved, the request is forwarded to the OPS Supervisor who reviews the request and forwards it to the SA. The SA changes the file/directory access privileges and then notifies the requester, supervisor and OPS Supervisor of completion.

Table 3.4-8, the **Activity Checklist** table that follows, provides an overview of the changing a file/directory access privilege process.

Table 3.4-8. Changing a File/Directory Access Privilege - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.7	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Supervisor.	(I) 3.4.7	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.7	
4	SA	Change a File/Directory Access Privilege.	(P) 3.4.7	
5	SA	Inform Requester, Supervisor and OPS Supervisor of completion.	(I) 3.4.7	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a file/directory access privilege has already been approved by the supervisor. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which access privileges will be changed**

b. **new access privileges to set on the file/directory. Can be any of:**

New owner

New group

New user/owner privileges (read, write and/or execute)

New group privileges (read, write and/or execute)

New other privileges (read, write and/or execute)

To change a file/directory access privilege for the requester, execute the procedure steps that follow:

1 At the UNIX prompt, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**.

- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.

4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type: (You must be /home) **chown *NewOwner* jdoe** and press **Return**.

5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type: **chgrp *NewGroup* jdoe** and press **Return**.

6 If there are **New user/owner privileges** then type **chmod u=*NewUserPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type: **chmod u=*NewUserPrivileges* jdoe** and press **Return**.

- The ***NewUserPrivileges*** are **r** = read **w** = write **x** = execute. To give the user/owner read, write and execute privileges, type: **chmod u=rwx *FileOrDirectoryName*** and press **Return**.

7 If there are **New group privileges** then type **chmod g=*NewGroupPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. ***Example:*** if the requester wants access privileges changed on directory /home/jdoe then type: (You must be in /home) **chmod g=*NewGroupPrivileges* jdoe** and press **Return**.

- The ***NewGroupPrivileges*** are **r** = read **w** = write **x** = execute.
  Example: to give the group read and execute privileges, type:
  chmod g=rx *FileOrDirectoryName* and press **Return**.

8 If there are **New other privileges** then **type:**
chmod o=*NewOtherPrivileges FileOrDirectoryName*, and press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chmod o=*NewOtherPrivileges* jdoe, and press **Return**.

- The ***NewOtherPrivileges*** are r for read, w for write and x for execute. For example, to give other read privileges, type:
  chmod o=r *FileOrDirectoryName* and press **Return**.

9 Type **exit**, press **Return**.

- Root is logged out.

To change a file/directory access privilege, execute the steps provided in the following table.

Table 3.4-9 contains a table which presents the steps required change a file/directory access privilege.

Table 3.4-9. Change a File/Directory Access Privilege - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**su**	**press Return**
2	***RootPassword***	**press Return**
3	**cd *Path***	**press Return**
4	**chown *NewOwner FileOrDirectoryName***	**press Return**
5	**chgrp *NewGroup FileOrDirectoryName***	**press Return**
6	**chmod u=*NewUserPrivileges FileOrDirectoryName***	**press Return**
7	**chmod g=*NewGroupPrivileges FileOrDirectoryName***	**press Return**
8	**chmod o=*NewOtherPrivileges FileOrDirectoryName***	**press Return**
9	**exit**	**press Return**

3.4.8 Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the OPS Supervisor. The OPS Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and OPS Supervisor.

Table 3.4-10, the Activity Checklist table that follows, provides an overview of moving a user's home directory process.

Table 3.4-10. Moving a User's Home Directory - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to OPS Supervisor.	(I) 3.4.8	
2	OPS Super	Approve/Deny Request in Accordance with Policy. Forward to SA if approved.	(I) 3.4.8	
3	SA	Move a User's Home Directory.	(P) 3.4.8	
4	SA	Inform Requester and OPS Super of completion.	(I) 3.4.8	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for moving a user's home directory has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New location for home directory**

To move a user's home directory for the requester, execute the procedure steps that follow:

3.5 Security

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. To monitor and control access to network services, ECS Security Services uses the public domain tool, TCP Wrappers. Three other public domain COTS products — npassword, Crack, and SATAN — provide additional password protection for local system and network access. The tool, Tripwire, monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for M&O Operations personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

3.5.1 Generating Security Reports

3.5.1.1 Reviewing User Activity Data

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file **/var/adm/loginlog**. The procedures assume that the file has been created and the operator has logged on as root.

Reviewing User Activity Data Procedure

1 At the UNIX prompt, type **/usr/bin/logins [-admopstux] [-g group..] [-l login..],** then press **Return/Enter**.

2 Type **logins -x -l *username,*** then press **Return/Enter**.

- Displays login status for a user:

3 Type **/var/adm/loginlog**, then press **Return/Enter**. To enable login Logging, this creates the log file **loginlog**.

4 Type **chmod 600 /var/adm/loginlog,** then press **Return/Enter**. This sets read and write permissions for root on the file.

5 Type **chgrep sys /var/adm/loginlog,** then press **Return/Enter**. This sets the group to **sys**.

3.5.1.2 Monitoring and Reviewing User Audit Trail Information

The **audit_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

/etc/security/audit_startup

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the audit_control file and re-initialize the current audit directory to the first directory listed in the audit_control file or to open a new audit file in the current audit directory specified in the audit_control file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

Audit Commands Procedures

1 **audit -n**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

2 **audit -s**, then press **Return/Enter**.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

3 **audit -t**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file, disable audit and die.

4 **praudit -sl** ***filename***, then press **Return/Enter**.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file /usr/include/sys/audit.h. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.

4. Database Administration

4.1 Overview of Database Administration

The Database Administrator or DBA, is the individual or group responsible for the installation, configuration, update, maintenance, and overall integrity, performance and reliability of the SQL Server database. In general, the DBA is concerned with the availability of the server, the definition and management of resources allocated to the server, the definition and management of databases and objects resident on the server, and the relationship between the server and the operating system.

4.1.1 ECS Database Environment

The database environment at ECS spans multiple databases serving numerous subsystems across several hosts. System Baseline Hardware/Database Maps, document 920-TD*x*-009-Rev*xx*, for the Distributed Active Archive Centers (DAACs) are available on the Pete.hitc.com website: http://cmdm.east.hitc.com. Select the "ECS Baseline" link button, and then the "Technical Documents" button to access this system data. The diagram, using ECS naming conventions, lists Subsystem identifiers (e.g., SUB – Subscription Server; SDSRV – Science Data Server; INGEST), the Host Platform (e.g., g0ins01, g0acg01, g0icg01), the Sybase Server designation (e.g., g0ins01_srvr, g0acg01_srver, g0icg01_srvr), the Database Names (e.g., SubServer, EcDsScienceDataServer1, Ingest), the various database component sizes (e.g., DB size, Log size, Index size), the Device Type (raw or filesystem) and the Database Owner Names (e.g., css_role, sdsrv_role).

In addition to the fundamental database design, ECS operates on a concept of mutually exclusive, functionally identical modes. The main mode that interacts with live data and customers is called the Operational mode (OPS). Other modes available at the DAACs are nominally called TS2, TS1, and SHARED. The SHARED mode contains files common to all modes. The TS2 and TS1 modes are used to implement and test new functionality for both COTS and CUSTOM code. After modifications are installed and successfully tested in a non-OPS mode, they are promoted to the next mode level and ultimately upgraded into the OPS mode. This concept enables uninterrupted operation for live data and user interaction while simultaneously field-testing new code. Figure 4.1.1-1 shows this multi-mode directory structure. The OPS mode is shown here and is identical for the TS2 and TS1 modes.

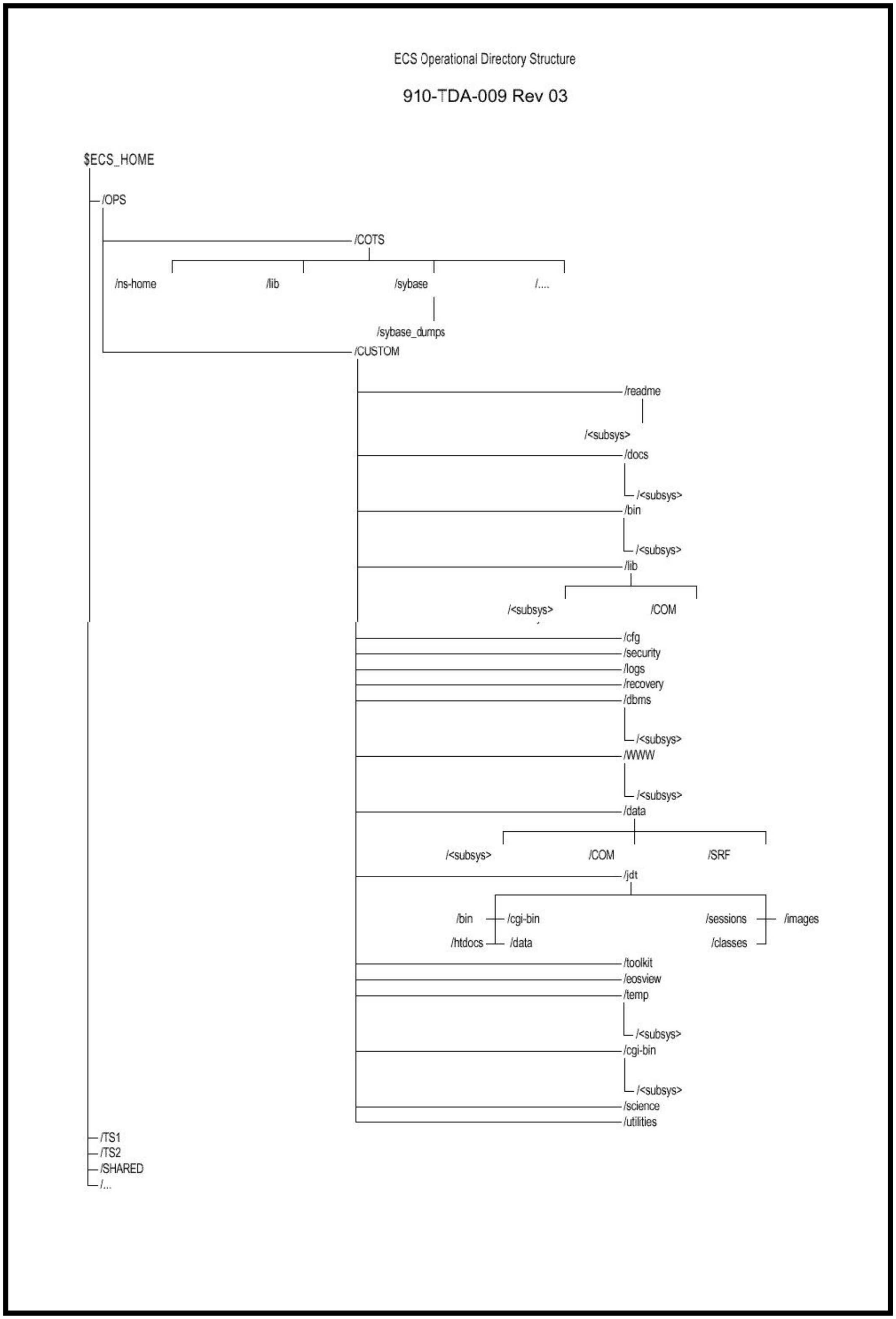


Figure 4.1.1-1. ECS Operational Directory Structure

4.1.2 Sybase Adaptive Server Enterprise

The version of Sybase Adaptive Server Enterprise (as well as other COTS software) installed on the SUN and SGI platforms is published in the COTS SOFTWARE VERSION BASELINE REPORT, 910-TDA-003-Rev*xx*. A more complete listing of software and the individual host installation content is provided in the DAAC-specific Hardware/Software Map, document 920-TDx-002-Rev*xx*. As upgrades are released and installed, version status will be reflected in these documents.

4.1.3 Database Schemas

All database designs in ECS are thoroughly documented in the 311 Series of documents, <SUBSYSTEM> Database Design and Schema Specifications for the ECS Project. These individual subsystem documents provide the DBA with a complete description of each database including:

Physical Data Model Entity Relationship Diagram

Tables

Columns

Column Domains

Rules

Defaults

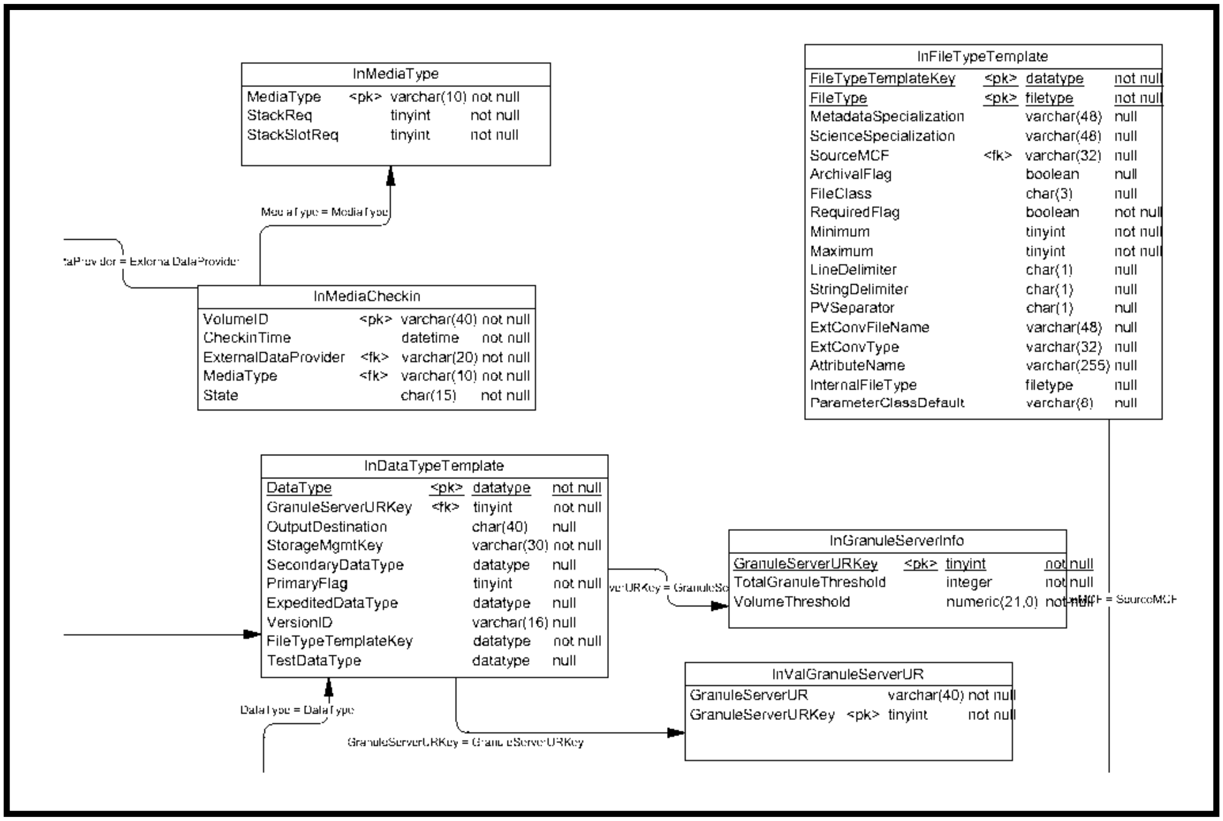
Views

Integrity Constraints

Triggers

Stored Procedures

The Schema documents also provide Performance and Tuning Factors, Database Security information, Scripts, and Entity Relationship Diagram Keys. Figure 4.1.3-1 is a portion of the Entity Relationship Diagram for the INGEST subsystem. To access this document, and the other subsystem 311 Series documents, use the following URL: http://edhs1.gsfc.nasa.gov/. From the ECS Data Handling Homepage select the “Document Catalogs” link and then the “Design Documents and Specifications” link. From this point you can select the relevant subsystem document.



InMediaType			
MediaType	<pk>	varchar(10)	not null
StackReq		tinyint	not null
StackSlotReq		tinyint	not null

InMediaCheckin			
VolumeID	<pk>	varchar(40)	not null
CheckinTime		datetime	not null
ExternalDataProvider	<fk>	varchar(20)	not null
MediaType	<fk>	varchar(10)	not null
State		char(15)	not null

InDataTypeTemplate			
DataType	<pk>	datatype	not null
GranuleServerURKey	<fk>	tinyint	not null
OutputDestination		char(40)	null
StorageMgmtKey		varchar(30)	not null
SecondaryDataType		datatype	null
PrimaryFlag		tinyint	not null
ExpeditedDataType		datatype	null
VersionID		varchar(16)	null
FileTypeTemplateKey		datatype	not null
TestDataType		datatype	null

InFileTypeTemplate			
FileTypeTemplateKey	<pk>	datatype	not null
FileType	<pk>	filetype	not null
MetadataSpecialization		varchar(48)	null
ScienceSpecialization		varchar(48)	null
SourceMCF	<fk>	varchar(32)	null
ArchivalFlag		boolean	null
FileClass		char(3)	null
RequiredFlag		boolean	not null
Minimum		tinyint	not null
Maximum		tinyint	not null
LineDelimiter		char(1)	null
StringDelimiter		char(1)	null
PVSeparator		char(1)	null
ExtConvFileName		varchar(48)	null
ExtConvType		varchar(32)	null
AttributeName		varchar(255)	null
InternalFileType		filetype	null
ParameterClassDefault		varchar(8)	null

InGranuleServerInfo			
GranuleServerURKey	<pk>	tinyint	not null
TotalGranuleThreshold		integer	not null
VolumeThreshold		numeric(21,0)	not null

InValGranuleServerUR			
GranuleServerUR		varchar(40)	not null
GranuleServerURKey	<pk>	tinyint	not null

Figure 4.1.3-1. Partial Entity Relationship Diagram - INGEST

4.1.4 DAAC Database Configurations

The key factors that determine optimum performance for any database are its configuration parameters. A document available on the Pete Server (http://cmdm.east.hitc.com), SYBASE SQL Server 11.0.x, ALL DAAC Database Configurations (910-TDA-021-Rev00), provides DBAs with detailed data and recommendations for Sybase configurable parameters. In addition to providing default values and the DAAC-specific parameter values for each host, it also describes the Sybase Segment naming conventions to be used at each site for assigning Sybase disk devices to databases. Future versions of this document will capture and baseline the disk devices at each DAAC and the interface file listings at each DAAC.

4.1.5 Database Disk Partitioning

System documentation also provides graphic depictions of server disk partitioning for all of the hosts (e.g. Ingest, MSS, CSS, PDPS DBMS). The 922-TDx-0xx-Rev00 series of documents (available on the PETE server) provide a block diagram of the disk partitioning for each of the servers (Figure 4.1.5-1) and also secondary tables (Figure 4.1.5-2) describing the physical break-down of the individual disks including Slice, Start Block, Total Blocks, Start MB, Total MB, XLV Name, Mount, and Type.

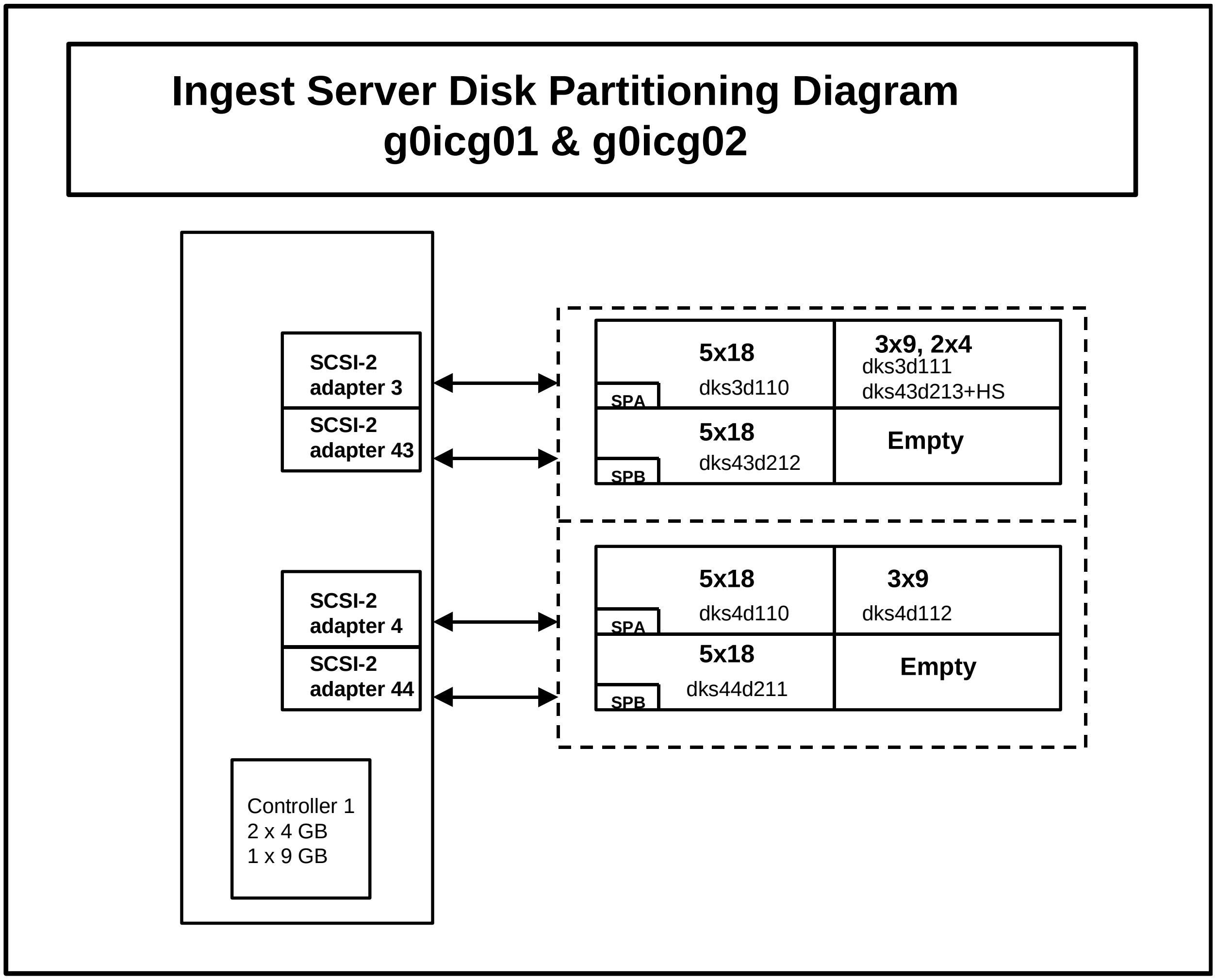


Figure 4.1.5-1. Server Disk Partitioning Block Diagram

dks3d111, 2x0 GB Raid Level 1, Mirrored

Slice	Start Block	Total Blocks	Start MB	Total MB	XLV Name	Mount	Type
0	2048	1024000	1	1	ingestlog		xlv
1	1026048	512000	501	501	sybsecurity		xlv
2	1538048	256000	751	125	sybmaster		xlv
3	1794048	512000	876	250	sybsecarchive		xlv
4	2306048	512000	1126	250	ddistlog		xlv
5	2814048	1024000	1376	500	stmgtlog		xlv
6	3842048	5120000	1876	2500	sybase_dumps		xlv
7	9862048	8264978	4376	4036	spare1		xlv
8	0	2018	0	1	n/a		Volhdr
10	0	17227026	0	8412	n/a		volume

Figure 4.1.5-2. Ingest Server Disk Partitioning Diagram

4.2 SQL Server Environment

4.2.1 Naming Conventions

As one of the most important, yet least applied concepts, naming conventions are presented in this chapter by examples according to the following rules.

Rule 1: Regardless of the length of the name, it should indicate the function and/or content of the object

Rule 2: Only easily understandable abbreviations should be used

Rule 3: Parts of names are separated by underscores "_", only one optional suffix is permitted (appended to the name by a . ".")

Rule 4: The full path of the object is considered to be part of the name

The names of the databases and tables themselves may or may not follow the above rules; these rules are specifically for the DBA to work with SQL Server objects, and files in the UNIX environment.

All **COTS** software is installed in the /usr/ecs/OPS/COTS directory.

All **SYBASE** software is located in the Sybase home directory (**$SYBASE**).

All backups are located in **$SYBASE**/sybase_dumps directory, which may or may not be on a separate physical disk.

Note:

It is strongly recommended that backups be stored on a separate physical disk.

The database dumps are kept for a period of 2 days and also stored on a disk by Networker everyday. The database dumps are named as follows:

dbname.dat_YYMMDDHHMM.Z

Where MMDDHHMM is the “sortable” eight digit month, day, hour, and minute. For example, on the date this chapter was written, a backup directory called backups_for_99021100024.Z

All SQL script files have the extension .sql as a suffix. Their names reference the objects they create or functions they perform, and are all located in $SYBASE/scripts.

SQL statement must follow precise syntactical and structural rules, and may include only SQL keywords, identifiers (names of databases, tables, or other database objects), operators, and constants. The characters that can be used for each part of a SQL statement vary from installation to installation and are determined in part by definitions in the default character set that version of the server uses.

For example, the characters allowed for the SQL language, such as SQL keywords, special characters, and Transact-SQL extensions, are more limited than the characters allowed for identifiers. The set of characters, which may be used for data, is much larger and includes all the characters that can be used for the SQL language or for identifiers.

The sections that follow describe the sets of characters that can be used for each part of a statement. The section on identifiers also describes naming conventions for database objects.

4.2.1.1 SQL Data Characters

The set of SQL data characters is the larger set from which both SQL language characters and identifier characters are taken. Any character in SQL Server's character set, including both single-byte and multibyte characters, may be used for data values.

4.2.1.2 SQL Language Characters

SQL keywords, Transact-SQL extensions, and special characters such as the comparison operators > and <, can be represented only by 7-bit ASCII values A- Z, a -z, 0-9, and the following ASCII characters:

4.2.1.3 Identifiers

Conventions for naming database objects apply throughout SQL Server software and documentation. Identifiers can be up to 30 bytes in length, whether or not multibyte characters are used. The first character of an identifier must be declared as an alphabetic character in the character set definition in use on Server.

The @ sign or _ (underscore character) can also be used. The @ sign as the first character of an identifier indicates a local variable.

Temporary table names must either begin with # (the pound sign) if they are created outside tempdb or be preceded by "tempdb..".

Table names for temporary tables that exist outside tempdb should not exceed 13 bytes in length, including the number sign, since SQL Server gives them an internal numeric suffix.

After the first character, identifiers can include characters declared as alphabetic, numeric, or the character $, #, @, _, ¥ (yen), or £ (pound sterling). However, you cannot use two @@ symbols together at the beginning of a named object, as in "@@myobject." This naming convention is reserved for global variables, which are system-defined variables that SQL Server updates on an ongoing basis.

The case sensitivity of SQL Server is set when the server is installed and can be changed by a System Administrator. To see the setting for your server, execute this command: sp_helpsort

4.2.1.4 Delimited Identifiers

Delimited identifiers are object names enclosed in double quotes. Using delimited identifiers allows you to avoid certain restrictions on object names. You can use double quotes to delimit table, view, and column names; you cannot use them for other database objects.

Delimited identifiers can be reserved words, can begin with non-alphabetic characters, and can include characters that would not otherwise be allowed. They cannot exceed 28 bytes.

Before creating or referencing a delimited identifier, you must execute:

set quoted_identifier on

The names of database objects need not be unique in a database.

However, column names and index names must be unique within a table, and other object names must be unique for each owner within a database. Database names must be unique on SQL Server.

If you try to create a column using a name that is not unique in the table or to create another database object such as a table, a view, or a stored procedure, with a name that you have already used in the same database, SQL Server responds with an error message.

You can uniquely identify a table or column by adding other names that qualify it, that is, the database name, the owner's name, and, for a column, the table name or view name. Each of these qualifiers is separated from the next by a period:

database.owner.table_name.column_name

database.owner.view_name.column_name

The same naming syntax applies to other database objects. You can refer to any object in a similar fashion:

If the quoted_identifier option of the set command is on, you can use double quotes around individual parts of a qualified object name.

Use a separate pair of quotes for each qualifier that requires quotes.

For example, use:

database.owner."table_name"."column_name"

rather than:

database.owner."table_name.column_name"

The full naming syntax is not always allowed in create statements because you cannot create a view, procedure, rule, default, or trigger in a database other than the one you are currently in. The naming conventions are indicated in the syntax as:

[[database.]owner.]object_name or: [owner.]object_name

The default value for owner is the current user, and the default value for database is the current database. When you reference an object in SQL statements, other than create statements, without qualifying it with the database name and owner name, SQL Server first looks at all the objects you own, and then at the objects owned by the Database Owner, whose name in the database is "dbo." As long as SQL Server is given enough information to identify an object, you need not type every element of its name. Intermediate elements can be omitted and their positions indicated by periods:

database..table_name

You must include the starting element, in this case, database, particularly if you are using this syntax when creating tables. If you omit the starting element, you could, for example, create a table named ..mytable. This naming convention prevents you from performing certain actions on such a table, such as cursor updates.

When qualifying a column name and a table name in the same statement, be sure to use the same naming abbreviations for each; they are evaluated as strings and must match or an error is returned.

4.2.1.5 Identifying Remote Servers

You can execute stored procedures on a remote SQL Server, with the results from the stored procedure printed on the terminal that called the procedure. The syntax for identifying a remote server and the stored procedure is:

[execute] server.[database].[owner].procedure_name

You can omit the execute keyword when the remote procedure call is the first statement in a batch. If other SQL statements precede the remote procedure call, you must use execute or exec. You must give the server name and the stored procedure name. If you omit the database name, SQL Server looks for procedure_name in your default database. If you give the database name, you must also give the procedure owner’s name, unless you own the procedure or the procedure is owned by the Database Owner.

If the server name in interfaces is in uppercase letters, you must use it in uppercase letters in the remote procedure call.

In all cases throughout this chapter, when actual examples are provided, those which reference UNIX commands will be preceded by a "%", and those that reference SQL statements will be preceded by a number and a ">" (e.g. 1>sp_help tablename).

The terms described in the following table will be used throughout this chapter.

Table 4.2.1-1. SQL Server General Definitions

Term	Definition
SQL Server	The server in the Sybase client/server architecture. SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.
Client	SYBASE Open Client software located in the /tools/sybOCv(TBD) directory for SUN and HP platforms SYBASE Open Client software located in the /tools/sybOCv(TBD) directory for SGI platform
Backup Server	Similar to the dataserver, it uses a separate UNIX process to off load the cycles associated with DUMP and LOAD commands
backups	The set of UNIX files containing full database dumps, transaction log dumps, and dbcc output
dbcc	Database Consistency Checker - a utility program designed to check the logical and physical consistency of a database
sybase root directory	/usr/ecs/OPS/COTS/sybase, this is the home directory for all SYBASE software and related products and is referenced both in UNIX and in the rest of this document as **$SYBASE**
interfaces file	Lists the names and access paths for all servers and backup servers. This file is located in the **$SYBASE**
sa	System Administrator login, this is the superuser of the SQL Server
scripts	UNIX script programs located in **$SYBASE**/scripts and related subdirectories {$ecs_Home}/{mode}/custom/dbms/{subsystem}
showserver	A utility invoked at the UNIX command prompt to display active servers, located in **$SYBASE**/install.
SQL scripts	SQL and command statements located in **$SYBASE**/scripts and related subdirectories and /{$ecs_Home}/{mode}/custom/dbms/{subsystem}
Server Name	The name of the database server for a specific application in different modes **EX. -** PDPS application database server in OPS mode EX.- Pdps_TS1 in TS1 mode EX. -pdps _TS2 in TS2 mode
Port Numbers	The port number to be utilized by the above listed servers.
Release Directory	$SYBASE
SQL	Structured Query Language

4.2.2 SQL Server Directory Structure

The **sybase** directory structure is described in the following table. Subdirectories under the **scripts** can contain template files with easy to modify examples of SQL and SQL command syntax.

Table 4.2.2-1. SYBASE Directory Structure

Directory	Contains
$SYBASE/bin	Utilities necessary to load, run, and access the server
$SYBASE /install	Files used to start and initialize dataservers, backupserver and to record server messages (errorlogs)
$SYBASE /lib	db-lib, ct-lib, and xa-lib client library files used by applications to gain access to the server (local to server) ***Applications use automounted libraries**.
$SYBASE /scripts	Root directory for all script files executed on the server
$SYBASE /sybase_dumps	Root directory that contains all backup subdirectories, it is recommended, but not required, that this directory be on a separate physical disk. Dumps both database and transaction logs. **Backups are stored on disk in the backup subdirectories.
backup subdirectories $SYBASE /sybase_dumps/dumps $SYBASE /sybase_dumps/trans $SYBASE /sybase_dumps/dumps/logs $SYBASE /sybase_dumps/trans/logs $SYBASE /sybase_dumps/Week1 $SYBASE /sybase_dumps/Week2 $SYBASE /sybase_dumps/Week1/logs $SYBASE /sybase_dumps/Week2/logs	A cron job is run at night to move data from the current (week1) directory to the previous (week2) directory. Then, a dump of the databases and transaction logs is executed and is stored in the current directory. All logs are written to the log directory. Files are saved using the following naming convention:: dbname.dat.YYMMDDHHMM.Z - full database dumps dbname.tran.YYMMDDHHMM.Z - full transaction log dumpsdbname_backup.log. dbname_ERR.log.MMDDHHMM - Error log filesdbname_dbcc.log. MMDDHHMM
**xxdmh02 serves as a remote Backup Server	**xx are the 2 letter codes to identify a DAAC site (i.e., g0 = Goddard)

4.2.3 SQL Server Installation

SYBASE SQL Server has been installed and configured by the ECS Installation Staff. Shared memory and disk resources have been allocated and configured by the System Administrator, and both the client and server portions have been set up by the DBA prior to shipment. Table 4.2.3-1 describes parameters and options used during installation.

Table 4.2.3-1. SQL Server Parameters and Options

Parameters Name	**Brief Explanation/Settings**
Retry Count	5 seconds
Retry Delay	5 seconds
Master device	28 Mb raw partition
Master Device Location	
Backup Server Name	SYB_BACKUP
sybsystemprocs	$SYBASE/devices/(MachineName)_sybprocs.dat, 19 Mb and on it's own device
Errorlog	$SYBASE/install/mode**.**errorlog (**mode** indicates the application)
Current default language	us_english
Current default character set	iso_8859-1 (Latin-1)
Current sort order	Binary ordering, for the ISO 8859/1 or Latin-1 character set (iso_1).
Internal auditing	On
sybsecurity database size	175 Mb - Varies – depends on disk allocations
sybsecurity device	sybsecurity, positioned on a 175 Mb raw partition

The installation script files are located in the **$SYBASE**/install directory. SQL Server installation is performed by an authorized user with the **sybinit** utility also located in the **$SYBASE**/install directory. See your UNIX System Administrator and the SYBASE SQL Server Installation Guide.

4.3 Database Administrator Responsibilities

The following subsections detail the most common functions that a DBA will perform.

4.3.1 Startup of SQL Server

Use **startserver** to start an SQL Server and/or a Backup Server. This command can only be issued by the **Sybase** user.

Syntax: % **startserver** [-f runserverfile]

The "runserverfile" is contained in the **$SYBASE**/install directory.

Note:

SQS server should be started after the SQL Server

4.3.2 Shutdown of SQL Server

Use **shutdown** to bring the server to a halt. This command can only be issued by the Sybase System Administrator (sa).

Syntax:1> **shutdown [backup_server_name]]** [with] [wait] [with nowait]

```
2> go
```

The "with wait" is the default option. This option brings SQL Server down gracefully.

The “with nowait” option shuts down the SQL Server immediately without waiting for currently executing statements to finish.

If you do not give a server name, shutdown shuts down the SQL Server you are using.

When you issue a shutdown command, SQL Server:

Disables logins, except for System Administrators

Performs a checkpoint in each database, flushing pages that have changed from memory to disk

Waits for currently executing SQL statements or procedures to finish

In this way shutdown minimizes the amount of work that automatic recovery must do when you restart SQL Server.

To see the names of the Backup Servers that are accessible from your SQL Server, execute

sp_helpserver. Use the value in the name column in the shutdown command. You can only shut down a Backup Server that is:

Listed in sysservers on your SQL Server, and

Listed in your local interfaces file.

Note 1:

It recommended that "with wait" option be used. This allows executing statements to finish.

Also it is recommended that you perform a checkpoint of all databases prior to shutdown.

Note 2:

SQS server should be started after the SQL Server

4.3.3 Showing SQL Server(s)

Use **showserver** to determine whether the SQL Server(s) and/or Backup Server(s) are running.

Syntax: % **showserver**

The “**showserver**” is contained in the **$SYBASE**/install directory

Example: UNIX processes running the various servers:

```
  UID   PID  PPID   C    STIME  TTY      TIME COMD
sybase   671    669   80   Apr 17    ?           80:05  /usr/ecs/OPS/COTS/Sybase/bin/dataserver    -d/dev/rdsk/c1t0d0s1 -g0sps06_srvr
sybase  665    663   80   Apr 17    ?          50:02  /usr/ecs/OPS/COTS/sybase/bin/backupserver
-g0sps06_backup -e/usr/ecs/OPS
```

4.4 Allocation of Resources

SQL Server can make reasonable default decisions about many aspects of storage management, such as where databases, tables, and indexes are placed and how much space is allocated for each one. However, the System Administrator has ultimate control over the allocation of disk resources to SQL Server and the physical placement of databases, tables, and indexes on those resources.

4.4.1 Creating Logical Devices

A logical device is created when the UNIX System Administrator determines that new disk space is available for use by SYBASE software, databases, transaction logs, and/or backups. Either raw disk partitions or UNIX filesystem partitions can be used to create a logical device. The creation of a logical device is a mapping of physical space to a logical name and virtual device number (**vdevno**) contained in the SQL Server **master** database. The **disk init** command is used to initialize this space. After the disk initialization is complete, the space described by the physical address is available to SQL Server for storage, and a row is added to the **sysdevices** table in the **master** database.

A System Administrator initializes new database devices with the disk init command.

Disk Init does the following: Maps the specified physical disk device or operating system file to a database device name

Lists the new device in master..sysdevices

Prepares the device for database storage

Note:

Before you run disk init, see the SQL Server installation and configuration guide for your platform for information about choosing a database device and preparing it for use with SQL Server. You may want to repartition the disks on your computer to provide maximum performance for your Sybase databases.

Disk init divides the database devices into allocation units of 256 2K pages, a total of 1/2MB. In each 256-page allocation unit, the disk init command initializes the first page as the allocation page, which will contain information about the database (if any) that resides on the allocation unit.

Note:

After you run the disk init command, be sure to use dump database to dump the master database. This makes recovery easier and safer in case master is damaged. If you add a device and fail to back up master, you may be able to recover the changes with disk reinit.

```
Syntax: disk init

name = "device_name" ,

physname = "physicalname" ,

vdevno = virtual_device_number ,

size = number_of_blocks

[, vstart = virtual_address ,

   cntrltype = controller_number]
```

4.4.1.1 Example of Creating a Logical Device

A raw partition on a RAID device has been made available to SQL Server by the UNIX System Administrator. Essentially, the actual name of the raw device **c2t0d1s3** has had it's ownership changed to **sybase** and it's group changed to **user**.

1. In **$SYBASE**/scripts/create.devices, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/OPS/COTS/sybase/scripts/create.devices

 % cp template.sql data_dev1.sql
```

2. Appropriate items are modified so that the script file resembles the following:

```
1> disk init

        2> name = “data_dev1”,

        3> physname = “/dev/rdsk/c2t0d1s3”,

        4> vdevno = 3,

        5> size = 128000

6> go

7> sp_helpdevice data_dev1

8> go
```

3. DBA runs the script from the UNIX command prompt:

Syntax: % isql -Usa -S**servername** -idata_dev1.sql -odata_dev1.out

4. DBA checks the data_dev1.out file for success

4.4.2 Creating and Altering Databases

A user database is created by the DBA with a script containing the **create database** command. A database is created on one or more physical devices. Specifying the device is optional - but highly recommended. When indicating the device, you use the logical name you specified as part of a **disk init** (described above). Unlike the **disk init** command, the size of the database data and log components is specified in MB instead of 2K pages.

4.4.2.1 Example of Creating a Database

The logical device **data_dev1** has been created (as above) along with another device called **tx_log1** (for transaction logging).

1 In **$SYBASE**/scripts/create.databases directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/OPS/COTS/sybase/scripts/create.databases

                    % cp template.sql userdb.sql
```

2 Appropriate items are modified so that the script file resembles the following:

```
1> create database UserDB on data_dev1 = 100 log on tx_log1 = 50 [with override]

         2> go

         3> sp_helpdb UserDB

         4> go
```

3 DBA runs the script from the UNIX command prompt:

Syntax: %isql -Usa -S**servername** -iuserdb.sql -ouserdb.out

4. DBA checks the userdb.out file for success

4.4.2.2 Example of Altering a Database

The user database **UserDB** has run out of space and it has been determined that it should be increased by 50MB.

1 In **$SYBASE**/scripts/create.databases, DBA creates a script file containing the ALTER DATABASE command (named alter_userdb.sql)

Syntax: Alter database UserDB on data_dev3 = 50

2 DBA runs the script from the UNIX command prompt:

Syntax: % isql -Usa -S**servername** -ialter_userdb.sql -oalter_userdb.out

3 DBA checks the alter_userdb.out file for success

4.4.2.3 Data Placement - Segmentation

Segments are named subsets of the database devices available to a particular SQL Server database. Segment names are used in **create table** and **create index** commands to place tables or indexes on specific database devices. Using segments allows the DBA to better control the size of database objects and may improve performance by spreading i/o more evenly across devices.

Once the database device exists and is available, the segment can be defined with the system stored procedure **sp_addsegment**.

Syntax: sp_addsegment segname, dbname, devname

After the segment has been defined in the current database, the **create table** or **create index** commands use the optional clause “on segment_name” to place the object on a particular segment.

```
Syntax: create table table_name (column_name datatype ...) [on segment_name]

        create [clustered | nonclustered] index index_name  on table_name (columns)
```

Use **sp_helpdb** database_name to display the segments defined for that database.

Use **sp_helpsegment** segment_name to list the objects on the segment and show the mapped devices.

4.4.2.3.1 Example of Creating a Segment

The DBA receives a request to create a segment for the storage of the DATA_INFO table indexes in the pdps_db_ops database, on a separate physical disk. Two devices **data_dev1** and **data_dev2** have already been created and are located on different physical disks.

1 In **$SYBASE**/scripts/create.segments directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/OPS/COTS/sybase/scripts/create.segments

        % cp template.sql segments_dev1.sql
```

2 The script file is modified so that it resembles the following:

```
1> sp_addsegment seg1_dev1, pdps, data_dev1

2> sp_addsegment seg1_dev2, pdps, data_dev2

3> go
```

3 DBA runs the script from the UNIX command prompt:

Syntax: %isql -Usa -S**servername** -ipdps_db_ops_segments.sql \

-opdps_db_ops_segments.out

4 DBA checks the pdps_segments.out file for success

5 When the table and indexes are created according to the instructions in section 4.4.6, the "on seg1_dev1" must be appended to the DATA_INFO.sql **create table** statement, and the "on seg1_dev2" must be appended to the DATA_INFO_indexes.sql CREATE INDEX statement.

Syntax: **create index** DATA_INFO_IDX on DATA_INFO (DI_ID) on SEG1_DEV2

4.5 Loading a Database You Have Created into a Different Database

Occasionally, you may want to create an exact copy of a database of you system. First, dump the existing database. Then create a database to load with this dump. The database does not have to be the same size as the original. The only requirement is that the destination database must be at least as large as the dumped database and have the same beginning fragments as the original database. This information can be obtained from saved database creation scripts, or by running the following command:

```
select segmap,'Size in MB'=size/512 from sysusages where dbid= db_id("database_name")
```

Example:

suppose your database was created with the following statement:

```
create database dbname on datadevice1 = 1000,
log on Logdevice1 = 200
go
alter device dbname on datadevice2 = 500
```

running:

```
select segmap,'Size in MB'=size/512 from sysusages
where dbid= db_id("dbname")
```

would return:

```
segmap  Size in MB
3       1000
4       200
3       500
```

You could create a 3GB database as follows and load your database into it (using "for load" option will shorten database load time):

```
create database newdatabase on datadevice3 = 1000 log on logdevice3 = 200
```

```
for load

go

alter database newdatabase on datadevice 3=500 for load go

alter database newdatabase on datadevice4=300 for load go

alter database newdatabase on datadevice5=1000 for load go

load database newdatabase from dbname_dump go
```

4.6 Monitoring Space Usage

4.6.1 Thresholds

Thresholds are defined on segments to provide a free space value at which a procedure is executed to provide a warning or to take remedial action.

Use **sp_addthreshold** to define your own thresholds:

sp_addthreshold database_name, segment_name, free_space, procedure_name

where free_space is the number of free pages at which the threshold procedure executes; procedure_name is the stored procedure which the threshold manager executes when the number of free pages falls below the free_space value. Please see the section on Auditing later in this chapter for an example of Thresholds.

Example of Threshold Commands mentioned above:

```
Sp_addthreshold CustomerDB, "default", 10230, CustDefaultSegWarn
```

4.7 Creating Database Objects

For special cases, creation (and modification) scripts are stored in **$SYBASE**/scripts/scriptname. There should be a template for each type of object to be created.

4.7.1 Example of Creating a User Table

The DBA has received a request to create a new table in the pdps_db_ops database called **PGE_Statistics** which has three column, pge_id, pge_statistic_type, and pge_statistic.

1. In the **$SYBASE**/scripts/create.db_objects directory, DBA creates a script file from the proper template.

```
 Syntax: % cd /usr/ecs/OPS/COTS/sybase/scripts/create.db_objects

 % cp table_template.sql PGE_Statistics_table.sql
```

2. Appropriate items are modified so that the script file resembles the following:

```
1> create table PGE_Statistics (
2> pge_id                  int,
3> pge_statistic_type  int,
4> pge_statistic           float )
        5> go
        6> sp_help PGE_Statistic
        7> go
```

3. DBA runs the script from the UNIX command prompt:

Syntax: %isql -Usa -S**servername** -iPGE_Statistics_table.sql \
-oPGE_Statistics_table.out

4. DBA checks the PGE_Statistics_table.out file for success

Other objects are created in like manner but are not included here due to space considerations.

4.8 Creating and Managing Logins and Roles

Earlier versions of SQL Server administrative responsibilities needed to be executed by and individual logged in –literally- as sa. Now specific user logins can be assigned components of administrative responsibility, enabling you to track and audit administrative activities.

The three roles are sa_role (systems administrator) for administrative tasks, sso_role(site security officer) for security tasks, and oper_rol (operator) for backup and recovery tasks.

In order to connect to a SQL Server a login must be created by the System Administrator or a system security officer. Login details are stored in the syslogins table in the **master** database.

The system stored procedure **sp_addlogin** adds new login names to the server but does not grant access to any user database.

Syntax: **sp_addlogin** login_name, password, [,default database ,language, fullname]

In order to gain access to a database, the System Administrator, system security officer, of the specific database owner must “add” the user with the **sp_adduser** system stored procedure.

Syntax: 1> **sp_adduser**login_name [username, group_name]
2> go

4.8.1 Example of Creating a Login and Granting Database Access

The DBA has received a request to authorize John Q. Public to the pdps_db_ops database.

***It is a good practice to have a default_db, when you create a user account.**

1. In the **$SYBASE**/scripts/create.users directory, DBA creates a script file containing the sp_addlogin command (named public.sql)

Syntax:

```
% cd /usr/ecs/OPS/COTS/sybase/scripts/create.users
% cp template.sql public.sql
```

2. DBA modifies appropriate fields so that the script resembles the following:

```
1> sp_addlogin jpublic,jpublic, default_db
2> go
3> use pdps (OPS mode)        4> go
5> sp_adduser jpublic
6> go
7> sp_helpuser
8> go
```

3. DBA runs the script from the UNIX command prompt:

Syntax: % isql -Usa -S**servername** - public.sql -opublic.out

4. DBA checks the public.out file for success

4.9 Permissions

Permissions are used to control access within a database. The DBA uses the **grant** and **revoke** statements to accomplish this. There are two types of permissions within a database, **Object** and **Command**. In general, **Object** privileges control select, insert, update, delete, and execute permissions on tables, views, and stored procedures. **Command** permissions control access to the **create** statements for databases, defaults, procedures, rules, tables, and views.

The syntax for the **grant** and **revoke** statements are quite similar:

grant {all [privileges] | command_list }

to { public | name_list | role_name }

revoke {all [privileges] | command_list }

from { public | name_list | role_name }

4.9.1 Example of Granting Privileges to a Specific User

The DBA receives a request that John Q. Public should be able to read the DATA_INFO table and read and update the SUBSCRIPTION_NOTIFICATION TABLE.

Syntax: 1> **grant** select on DATA_INFO to jpublic

```
        2> grant select, update on SUBSCRIPTION_NOTIFICATION to jpublic
go
```

Note: It is recommended that the DBA store these command in a “.sql” file in the **$SYBASE**/scripts/create.db_objects directory, along with their results.

4.10 Backup and Recovery

Table 4.10-1. Backup and Recovery Definitions

Term	**Definition**
Backup Script Components	Located in the **$SYBASE** directory, they include: sybasedump, dmpdb_trns, copy_daily_dumps_to_week1, copy_daily_dumps_to_week2
Backup files	Defined in Table 4.2-2, the location of these files has been determined during server setup
Backup Statements	Generated from the sql in sybasedump these include calls to dbcc, Dump Database, and Dump Transaction commands
Backup Subdirectory	The only directory level underneath of the Backup Directory, defined in Table 4.2-2.
Backup Summary	An extraction of the successful Dump messages along with any errors generated by the Backup Statements stored in the Backup Subdirectory.

4.10.1 Automatic Backups

The following list identifies all procedures and scripts files that are currently being used for Sybase backups. There are cron jobs running at all sybase **servers** that have SQL server installed. All dump files are currently written to LOCAL machine. The site DBA is responsible for configuring the backup dump to the REMOTE sybase directory.

To check if the crontab is up and running, enter:

```
> crontab -l
```

Example of the output:

```
019  * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb

012 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran

021 * * 1-5 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog
```

NOTE:

If the crontab is not running enter:

```
                > crontab   /usr/ecs/OPS/COTS/sybase/run_sybcron
```

The following files will be installed by EcCoAssist to the /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin directory:

EcCoDbSyb_README

EcCoDbSyb_DumpDb

EcCoDbSyb_DrumpTran

EcCoDbSyb_DbStat

EcCoDbSyb_SedFile

EcCoDbSyb_DboMail

EcCoDbSyb_SetupKsh

EcCoDbSyb_CkErrorLog

EcCoDbSyb_tran_log.awk

SCRIPTS	DESCRIPTIONS
EcCoDbSyb_SetupKsh	This file contains the SYBASE and DSQUERY (server) environment setup. This file is call by EcCoDbSyb_DumpDb, EcCoDbSyb_DrumpTran, and EcCoDbSyb_CkErrorLog scripts.
EcCoDbSyb_DumpDb	This script contains the code to dump the databases. First, it checks for any DBCC error on the master database, if there is any error on the master, the script sends an email to the DBA and exit the program. If the master database dump was successfull, then the rest of the databases are dumped. Each database has a DBCC check, if there is any error on the database then the database is NOT dumped and an email is send to the DBA. At the end, an status email is send, providing all the database names that were succefully dumped
EcCoDbSyb_DumpTran	This script contains the code to dump the transaction logs. This dumps the transaction logs for each database, it check the error log file, if the error Msg is 4207 or 4221 it will do a dump of the database firt, then it will do the trasaction dump. If there is any other error Msg then the transaction dump will fail and email will be send. At the end, an status of the transaction log dumps is email to the DBA
EcCoDbSyb_SedFile	This file contains all the database that don’t need to be dump (i.e., temp, model, etc.)
EcCoDbSyb_DboMail	This file contains the email list of all the DBA’s.
EcCoDbSyb_DbStat	This script updates the index table of a database. This script is called from EcCoDbSyb_DumpDb after each successfully database dump.
EcCoDbSyb_CkErrorLog	This script checks for specific database error messages from the Sybase Error Log File every hour and emails the error messages to the DBA’s in the EcCoDbSyb_DboMailfile.
EcCoDbSyb_tran_log.awk	This script matches the current hour with the hour the error messages were enerated in the Error Log File. If errors found, the messages are saved in a mailfile and sent to DBA’s.

THE FOLLOWING FILES MUST BE MODIFIED BEFORE RUNNING ANY OF THE ABOVE SCRIPTS:

EcCoDbSyb_SetupKsh	Make user you have the SYBASE files under /usr/ecs/OPS/COTS/sybase
EcCoDbSyb_SedFile	Add any other database that might not need to be backed up. The databases that are listed in this file do not need to be backed up.
EcCoDbSyb_DboMail	Add/delete the email of the DBA and any other email that might need to be added/deleted. All the errors and status will be send to them.
run_sybcron	The following is an example on the crontab file that should be run by a sybase user. The first one will run the EcCoDbSyb_DumpDb script that dumps the databases at midnight from Monday to Saturday. The second one, EcCoDbSyb_DumpTran script that dumps the transaction logs will run tree times a day, 10AM, 1PM and 4PM from Monday to Saturday. The Third one, EcCoDbSyb_CkErrorLog that check the SYBASE error log file will run every hour from Monday to Saturday.

```
0 0  * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb
0  10,13,16 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran
0 * ** 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog
```

NOTE: Make sure there is an OPS mode directory with all script files.

All these scripts reside in "/usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin" directory. The assigned site DBA will be responsible for maintaining, modifying and applying necessary changes that are applicable to their site as for (security, and backup schedule).

SQL Server backups are performed nightly by a **cron** job which runs the **run_sybcron** program located in the **$SYBASE**/ directory. The following table of definitions will be used throughout the rest of this section.

Table 4.10.1-1. Automatic Backup Components

Component Name	**Function(s)**
run_sybcron	File added with the crontab -e command, contains several executable cron commands. **Example:** 00 19 * * 1-6 /data1/COTS/sybase/sybasedump
EcCoDbSyb_DumpDb	Controlling script that performs the following functions: run isql to create the Backup Statements run isql to execute the Backup Statements record the results of the Backup Statements in Backup Files copy the Backup Files to the Backup Subdirectory create the Backup Summary "greps" successful Dump statements along with any errors generated, sends e-mail to the DBA and writes them to the backup_summary file
sp	SQL Server password file - contains password for backup role

No intervention in the Automatic Backup Process is required by the DBA, though periodic checks of the Backup Subdirectories are recommended.

4.10.2 Manual Backups

Manual backups can be performed at any time by the System Administrator and are recommended for the following situations:

Any change to the **master** database - this includes new logins, devices, and databases

Any major change to user databases - a large ingest or deletion of data, definition of indexes

Other mission-critical activities - as defined by the DAAC Operations Supervisor.

Both the **dump database** and **dump transaction** command processing are off-loaded to the backup server, and will not affect normal operations of the database. These commands are performed by the System Administrator on appropriate databases as follows:

Syntax:

1> dump database master to
"/usr/ecs/OPS/COTS/sybase/sybase_dumps/dumps/dbname.dat.MMDDHHMM."

go

After dumping the database, compress the dump file by executing:

```
        %compress
/usr/ecs/OPS/COTS/sybase/sybase_dumps/dumps/dbname.dat.MMDDHHMM.
```

Syntax:

```
dump transaction pdps_db_ops to
“/usr/ecs/OPS/COTS/sybase/sybase_dumps/trans/pdps_OPS.tran.YYMMDDHHMM"”

go
```

4.10.3 Manual Recovery

Manual recovery of a user database is performed by the System Administrator by the use of the **load database** and **load transaction** commands. For issues concerning the **master** database, please consult your System Administrator’s Guide for assistance. It is recommended that any user database to be recovered be dropped and created with the **for load** option., The **databasename**.sql along with any **alter.databasename**.sql scripts can be , combined into one script which will re-create the user database with the **for load** option. This will insure the success of the **load database** and **load transaction** commands.

4.10.4 The BulkCopy Utility

The **bcp** utility is located in the **$SYBASE**/bin directory and is designed to copy data to and from SQL Server databases to operating system files.

4.10.4.1 Requirements for Using bcp

In general, you must supply the following information for transferring data to and from SQL Server:

Name of the database and table

Name of the operating system file

Direction of the transfer (in or out)

In order to use **bcp**, you must have a SQL Server account and the appropriate permissions on the database tables and operating system files that you will use. To copy data **in**to a table, you must have **insert** permission on that table. To copy data **out** to an operating system file, you must have select permission on the following tables:

The table being copied

sysobjects

syscolumns

sysindexes

bcp Syntax

```
bcp [[database_name].owner.]table_name {in | out} datafile [-e errfile] [-n] [-c]
        [-t field_terminator] [-r row_terminator] [-U username] [-S server]
```

4.10.4.2 Example of User Database Recovery

The database **UserDB** was created using the following script excerpt: (stored in home/scripts/create.databases/userdb.sql)

create database UserDB on data_dev1 = 100 log on tx_log1 = 50 [with override]

and was modified using the following script excerpt: (home/scripts/create.databases/alteruserdb.sql)

Alter database **UserDB** on data_dev1=50

For the purposes of this example, the full database backup and transaction log dumps were successful and located in /usr/ecs/OPS/COTS/UserDB.dat and UserDB_tx.dat

1. In the **$SYBASE**/scripts/create.databases directory, DBA makes a script file from the template.

```
Syntax: % cd /usr/ecs/OPS/COTS/sybase/scripts/create.databases
                % cp template.sql userdb_for_load.sql
```

2. Appropriate items are modified so that the script file resembles the following:

1> create database UserDB on data_dev2=100 log on tx_log2=50 **for load**

2> go

3> alter database UserDB on data_dev3=50

4> go

3. DBA saves the script in $SYBASE/scripts/create.databases/userdb_for_load.sql

4. DBA runs the script from the UNIX command prompt.

Syntax: %isql -Usa -S**servername** -iuserdb_for_load.sql -ouserdb_for_load.out

5. DBA checks the userdb_for_load.out file for success

6. DBA loads the database from the full backup.

Syntax: 1> load database UserDB from

“/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.dat.MMDDHHMM”

go

7. DBA loads the transaction file from the transaction file dump.

Syntax: 1> load transaction UserDB from

“/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.tran.MMDDHHMM”

3> go

4.11 Database Performance and Tuning

Once your application is up and running, the DBA monitors its performance, and may want to customize and fine-tune it. Use the following software tools provided by SQL Server:

Setting query processing options with the **set** command

Setting database options with **sp_dboption**

Monitoring SQL Server activity with **sp_monitor**

Using **update statistics** to ensure that SQL Server makes the best use of existing indexes

Changing system variables using **sp_configure** and the **reconfigure** command

Placing objects on segments to spread i/o, improve throughput, etc. as described in section 4.4.4

For a complete discussion of issues related to SQL Server performance and tuning, refer to your SYBASE SQL Server Performance and Tuning.

4.12 Installation of the Applications

DBA should have physical devices configured before installing either autosys or remedy. Both applications use Sybase as their database.

4.12.1 Installation of the Application Database

The installation of the application databases has been automated using ECS Assistant. The application databases are created using the DbBuild script which can only be invoked through ECS Assistant or the Command Line. Scripts that ECS Assistant invokes are:

DbBuild - Create new empty database and loads with initial data.

DbPatch - Upgrade to new schema while retaining existing data.

4.12.2 The AUTOSYS Application and other Configuration Issues

The AUTOSYS application works in tandem with PDPS/DPSs to schedule the jobs that run on Science Processor. Autosys installation is performed in /usr/ecs/OPS/COTS by the auto install program located in the autosys/install directory. The results of the installation are stored in an autosys_install.scr file located in the AUTOSYS home directory (/use/ecs/OPS/COTS/autosys). For pdps to run properly with AUTOSYS, the following activities are completed:

A user is defined named **autosys**

autosys user is added to the pdps database (OPS mode)

The autosys server is added to the sysservers table with **sp_addserver**

The server is added to the sysservers table on the AUTOSYS server with **sp_addserver**

4.12.3 Spatial Query Server (SQS)

SQS is a multi-threaded, Sybase Open Query database engine, which is required by the Science Data Subsystem (SDSRV). This product allows definition of spatial data types, spatial operators, and spatial indexing. SQS communicates with Sybase SQL Server to process SDSRV requests to push and pull metadata. SDSRV database server resides on an SGI machine. SQS also, reside on the same machine as SDSRV Sybase SQL Server.

Named X1acg01 - where X is the DAAC specific identifying character.

pathname - /usr/ecs/OPS/COTS/sqs222/bin/sqsserver

Should have one dedicated CPU per instance running. Defaults to one instance now, but may require additional instances later for performance reasons.

Requires one entry in the Sybase “interfaces” file per instance of the SQS server to be run.

Consult startup scripts in /etc/init.d/sybase and /etc/init.d/sqs_222

SQS requires a Sybase login with SA or sa_role and associated password to start. SQS environment variables requirements:

SYBASE = Location of the Sybase home directory. Example: /tools/sybOCv(TBD)

PATH = Must include in this order - /usr/bin; /usr/sbin;$SYBASE/bin

DSQUERY = Name of SQL Server to which to connect. From the $SYBASE/intefaces file. Examples - g0acg01 _srvr

DSLISTEN = Name of SQS server to use. Example - g0acg01_ srvr

SQSUSER = Name of the user (SA or sa_role) for system connection.

SQSPASSWORD = Password for the system connection login

The SQS startup script requires the following information:

SQSHOME = location of sqsserver binaries.

The following is a list of options that can be imbedded in the startup script, these options are beneficial, but they are not required.

4.12.3.1 SQS Startup Options

-e path of the SQS server logfile. Example /usr/ecs/OPS/COTS/sqs222/sqs/bin/sqs_222.log

-u number of concurrent SQS connections. Recommend minimum of 125. Example -u 125

Usually started with a delay, after the SQL Server is started. This delay be sufficient for the SQL server to recover and come-up.

$SQSHOME/bin/sqsserver -e $SQSHOME/sqs_222.log -u $USER &

SQS has dependencies on Sybase, such as:

Sybase must be running prior to starting SQS

SQS user id that starts SQS, which is different from the application user ID must have admin privileges

SQS opens a connection to Sybase's because it writes to the Sybase System tables

SQS server thread runs under the userid sa. In order to avoid confusion when monitoring this thread, it is best to:

create a separate login and userid specifically to monitor SQS

grant sa_role authority to the userid created to monitor SQS

EXAMPLE: 1> **sp_adduser** sqs_mon

grant sa_role to sqs_mon

go

4.13 Configuration of XLV Partitions for Sybase Partitions

In order to successfully convert the raw partitions using the logical volume disk driver (XLV), the following steps are to be strictly adhered to.

BACKUP all databases.

BCP the syslogins table from master.

bcp master..syslogins out file.out -Usa -P -c

bcp master..sysloginroles out file.out -Usa -P -c

Save all information regarding the sysdevices and database options by executing the following command:

sp_helpdb db_name -- each database

sp_helpdevice

sp_helpdb

Shutdown the backup and sql servers.

After the partitions have been updated to XLV, chown the sybase disks to sybase:users. Also, change the /etc/init.d/sybase script.

Cleanup some old sybase files from $SYBASE/devices and $SYBASE/install.

Execute sybinit to initialize a NEW sql server/backup (same server name).

Initialize sybsystemprocs database, as well.

Change sa password. (sp_password NULL,newpass)

Up the number of devices. (sp_configure "number of devices",20)

alter the database for master and tempdb.

Change sysservers to name the server, as well as the new backup server.

sp_addserver nodename_srvr,local,nodename_srvr

sp_addserver SYB_BACKUP,local,nodename_backup

execute scripts to initialize the devices and to create databases (for load).

load database dumps. Verify that database data and log are not on same device. If on same device, update sysusages by deleting the log that uses he data device and then update the size of the data device to the full size (plus the one used by the log).

uncompress the load file, manually.

online database

BCP in the syslogins table

BCP in the sysloginroles table

Change the DB dbo

Reset all DB options

Dump all databases.

4.13.1 Backout Procedure

This is an addendum to the technical directive that was previously sent out, dated September 28,1999. The backout procedure is executed only if it is necessary to restore the old SQL server because of a XLV conversion failure.

After restoring the sybase raw disk partitions from XLV partitions (normally done by the System Administrators), change the ownership of the devices to sybase:user. This step has to be executed by someone with root access.

Login as sybase, and cd to the $SYBASE/install directory.

Execute sybinit and configure a new sql server. Use the same configurations that were used from original sql server, ie. Port numbers.

Once you have configured a new server, get in to isql and execute the following:

change sa password

alter database master to same size as before

modify the sysservers with the sql and backup names

shutdown sql server and bring it up in single user mode (-m option)

uncompress the master database dump (do not load at this time)

cd to /usr/ecs/OPS/COTS/sybase/devices and copy the old sybsystemprocs.dat to the new one

load the dump of the master database (after the load, it would automatically shut down the sql server, so, start it up as normal and not as single user)

Now, at this point, all your databases should recover. If not, your databases would be marked as suspect. Then, check your devices and load each database from the dumps. Just follow the following steps:

Check all the devices and make sure that they do exist

Drop the databases using dbcc repair (dbname,dropdb) option

Re-create the databases with a “for load” option

Load each of the databases and do an online command after

Verify that your db options were set properly, as well as all the users on each database

Once, everything is back to its original state, do a complete backup of all your databases!

This completes the backout process.

4.14 Passwords Security

Security has become a sensitive issue throughout the Information Technology (IT) Industry. The ECS program is also concern about security and the risks associated with security. As a result the following directive is issued to all DAACs.

All System Administrators and Database Administrators at the sites are responsible for reasonable security measures when installing ECS custom software. This means:

Changing the permissions of online secure files to the minimum level required .

Backing up secure file(s) to removable media (floppy or tape) and removal of secure files immediately after installation is complete.

1. The media should then be kept in a secure location.

The following file is affected as result of this requirement on the ECS program.

A. /usr/ecs/<MODE>/CUSTOM/dbms/<SUBSYSTEM>/Ec<server>SybaseLogins.sql

B. Set permissions to 711 (user read, write, execute, group and other read only)

4.15 ECS Sybase Replication Server Administration Overview

Sybase Replication Server was used for the ECS Project starting in release 6A. Implementation of Replication Server for Earth Observing System Distributed Information System (EOSDIS) Core System (ECS) will require the support of the Management Subsystem (MSS). The deployment of the Sybase Replication software and its support tools that distributes data across distributed active archive center (DAACs) imposes additional operational requirements beyond original concept of a stand-alone DAAC operations. This new concept will allow all science users to register only once at their specified Home-DAAC and be able to request data from all DAAC sites.

Sybase Replication Server's most basic model is the “primary copy model.” In this model, database transactions are replicated from the primary database (locate at the System Monitoring Center) to a replicate database via one or more replication servers. The model assumes ‘ownership’ of the data by the primary database. This means, the data can only be updated by clients (local DAACs) connected to the primary database and that clients connected to the replicate database have read-only access to the data.

The transactions are continuously replicated asynchronously from the primary to the replicate database. Replication is transparent to client applications that submit database transactions to the primary database. However, this feature creates a latent period (the time it takes to propagate the transaction across the network) during which data in the primary and replicate databases are inconsistent with each other. Client programs using these databases must account for this latency.

Sybase Replication Server implements this model using replication definitions for tables at the primary database and subscriptions for tables at the replication definitions. The replication definitions specify the location of the primary data while the subscription specifies the location of the replicate data. The replication definition and subscriptions are specified at the table or stored procedure level. Replication does not require replicating all tables in a database.

The primary copy model can be viewed as a building block to create other models. The model attempts to prevent data inconsistencies that would be created by updating and replicating copies of the same data in two databases simultaneously. The model stipulates that inserts, updates, and deletes to the data can only occur at the primary database, while select statements may occur at either the primary or the replicate database. The model assumes the enforcement of data ownership using custom developed database triggers, client code, or operational procedures.

The deployment of software that distributes data across distributed active archive center (DAAC (s)) imposes additional operational requirements beyond stand-alone DAAC operations. These enterprise level requirements conflict with the requirements for autonomous DAAC operations in two major areas: 1) capabilities that rely on database replication will be temporarily disabled between DAACs if the databases and/or software are at different schema/drop levels; 2) administration of replicated databases requires coordination between DAACs.

This document focuses on the operations and administration of a replication system in a multi-site configuration by examining several operation scenarios involved in replication software installation and Replication Server administration. Although Sybase Replication Server (RS) supports same-site replication for warm-standby or load balancing needs, this document will focus exclusively on the issues involved in administering Sybase Replication Server for cross-site data distribution.

4.15.1 Cross DAAC Primary Copy Model Components

Figure 4.15.1-1 illustrates the components used in a primary copy model that uses two replication servers. This example is for illustrative purposes only. The ECS implementation will be described in the next section.

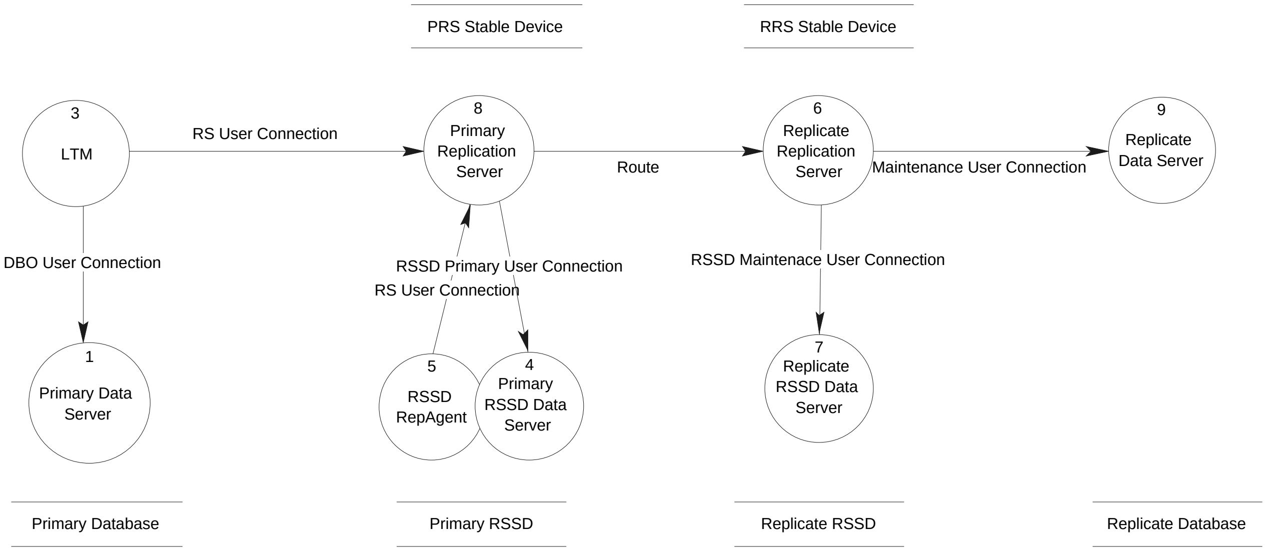


Figure 4.15.1-1. Replication Server Components

Components:

DAAC Component	Description
Primary Data Server	The primary data server is the Sybase SQL server that maintains the primary copy of data that is being replicated.
Primary Database	Contains the copy of data that can be updated by application programs.
LTM	The log transfer manager (LTM) is a Sybase Open Server application that transfers replicate database transactions to a primary replication server and moves the secondary truncation point in the primary database transaction log. The LTM connects to the primary data server as the primary database DBO and to the primary replication server as specified when the primary database is added to the domain.
Primary Replication Server	The primary replication server (PRS) is responsible for forwarding replicate database transactions to the replicate database. The PRS maintains connections to the replicate replication servers (route) and maintains a connection to its database, the Replication Server System Database (RSSD).
Primary RSSD Data Server	The primary RSSD data server maintains the primary RSSD.
RSSD RepAgent	The RSSD RepAgent is a thread in the primary RSSD data server that transfers replicate RSSD database transactions to the PRS. The RSSD RepAgent connects to the PRS as specified when the PRS is added to the domain.
Primary RSSD Database	The RSSD houses the information required by the replication servers to operate.
PRS Stable Device	The PRS stable Device contains a First In First Out (FIFO) queue for each primary and replicate database. Transactions are transferred from a primary database queue to a replicate database queue after the LTM sends the transaction’s commit. Once a transaction is moved to the replicate database queue, the primary replication server sends the transaction to the replicate replication server.
Replicate Replication Server	The replicate replication server (RRS) is a replication server that receives replicate transactions from a primary replication server and applies the transaction to a replicate database. The RRS maintains a maintenance user connection for each replicate database.
Replicate RSSD Data Server	This server houses the RSSD for the RRS.
Replicate RSSD	This database contains information that is required for the RRS to apply replicate database transactions to a replicate database.
RRS Stable Device	The RRS stable device is a file system that contains a FIFO queue for each replicate database. Replicate database transactions are pushed into the queue before being applied to the replicate database.
Replicate Data Server	This server houses the replicate database and is updated by the RRS.
Replicate Database	The database that contains the replicate data.

4.16 Overview of Replication Design

In the current system design, the System Monitoring and Coordination Center (SMC) database is the primary database for all records. This means that all account request, profile creation, and profile modification activities must take place at the SMC. Sybase replication automatically sends database changes from the SMC to the other sites once they are committed. This significantly reduces the interval from the time a change is made to the time in which that change is propagated to other sites. Figure 4.16-1 illustrates replication for the User Profile database.

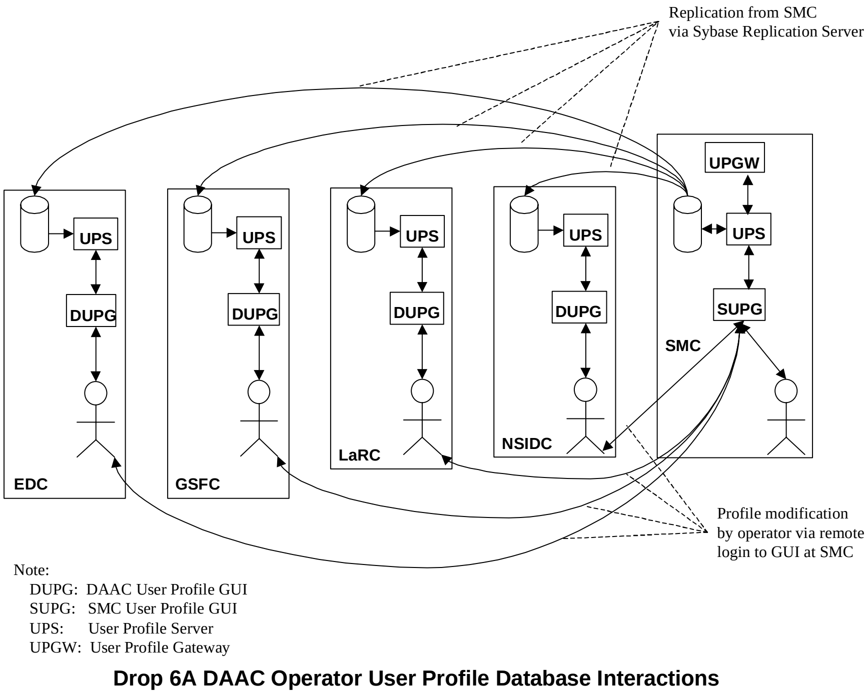


Figure 4.16-1. DAAC Operator User Profile Data Interactions

4.16.1 Ground Data System (GDS) Order Tracking

The GDS gateway is located at the System Monitoring Center (SMC) and supports ASTER GDS submitted cross-DAAC product requests and product request status queries. Product requests are routed to and processed by the appropriate DAAC. The DAAC filling the request updates a local copy of the request tracking data. The request tracking data is replicated to EDC to support the product request status queries submitted via the GDSGW.

Since a product order may contain several requests, the order and request information stored at SMC contains all requests processed at one or more DAACs. On the other hand, the DAAC processing the request contains only its portion of the request(s) for the order.

This requirement imposes an inconsistency in the order data between sites, since the order data is a summation of requests. GDS order tracking has a requirement to preserving the order information, independent of individual DAAC operations. The requirement stipulates that request delete transactions are **not** replicated back to EDC.

4.16.2 User Profile Distribution and User Registration Interaction Flow

Figure 4.16.2-1 depicts the User Registration Interaction Flow. As the figure suggests, a science user who wishes to become a registered user associated with a particular DAAC (the Home DAAC) submits a New User Request (A.1). The user employs the User Registration Tool to submit the request to the User Registration Server at the SMC (A.2) The New User Request is retrieved by the User Services Representative at DAAC operations, logged in to the SMC remotely and using the Account Management tool (A.3). Note that the representative sees only requests specifying that representative's DAAC as Home DAAC are available to that representative for review. The representative reviews the information in the request and completes the User Profile (A.4). Upon completion of the User Profile at the SMC, the system sends confirmation to the user (A.5). With secure transmission of information, it is possible to send information electronically for printing of the User Profile information, including password, to the DAAC, so that the information can be printed and sent to the user by surface mail (A.6). The replication process (A.7) ensures that each DAAC has the entire User Profile database available on the local User Registration Server for viewing.

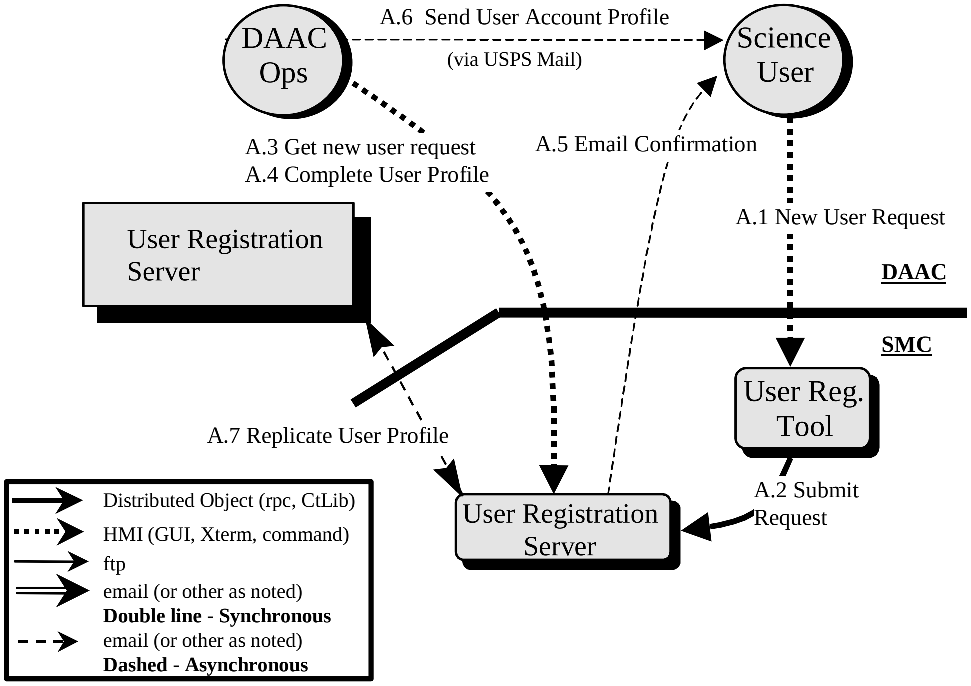


Figure 4.16.2-1. User Registration Interaction Flow Diagram

4.16.2.1 User Registration Interaction Table - High-Level Operational View

Table 4.16.2.1-1 provides the Interaction - High-Level Operational View: User Registration.

Table 4.16.2.1-1. Interaction Table - High-Level Operational View: User Registration (1 of 2)

Step	Event	Interface Client	Interface Provider	Data Issues	Step Preconditions	Description
A.1	New User Request	Science User	User Registration Tool	None	None	Science user loads User Registration Tool, via its URL, from a favorite Web Browser. Science user fills out form with initial registration information. This information includes: user name, address, telephone number, email address, and user verification key (for security confirmation). Request is queued at the SMC.
A.2	Submit Request	User Registration Tool	User Registration Server	None	None	User Registration Tool submits the new user's request. The request is queued at the SMC, awaiting the DAAC User Services staff from the user's selected home DAAC o confirm the new user.
A.3	Get New User Request	DAAC User Services Representative	User Registration Server	None	None	DAAC User Services Representative (periodically) checks for new user registration requests. In this case the request for our new user is found. User Services staff checks the information provided.
A.4	Complete User Profile	DAAC User Services Representative	User Registration Server	None	None	DAAC User Services Representative completes the new user's User Profile. The request is marked as confirmed and accepted. DAAC User Services Representative may call Science User for any further information or clarification. The Representative may authorize any special privileges (e.g., access to restricted granules, submission of ASTER Data Acquisition Requests) at this time.

Table 4.16.2.1-1. Interaction Table - High-Level Operational View: User Registration (2 of 2)

Step	Event	Interface Client	Interface Provider	Data Issues	Step Preconditions	Description
A.5	Email Confirmation	User Registration Server	Science User	None	None	User Registration Server e-mails confirmation of the user’s registration request.
A.6	Send User Account Profile	DAAC User Services Representative	Science User	None	None	DAAC User Services Representative sends complete user account profile, including user name and password, to Science User via USPS mail.
A.7	Replicate User Profile	Sybase	Sybase	None	None	The user profile is replicated at each DAAC. Each DAAC is capable of browsing user profiles locally. User profiles can only be created or modified at the SMC by operators from the user’s home DAAC (who logs in remotely) or by select SMC operators.

4.16.2.2 User Registration Component Interaction Table

Table 4.16.2.2-1 provides the Component Interaction: User Registration. The information in this table provides more detail on specific interactions among ECS components for each of the main elements identified in Table 4.16.2.1-1 for those interested in what is occurring between ECS software configuration items and their components during user registration processes.

Table 4.16.2.2-1. Component Interaction Table: User Registration (1 of 2)

Step	Event	Interface Client	Interface Provider	Interface Mech	Description
A.1.1	Startup User Registration Tool	Science User	EcClDtUserProfileGateway	Web Browser	Science User invokes the configured Web Browser with the URL of the User Registration Tool.
A.1.2	Input User Registration Information	Science User	EcClDtUserProfileGateway	Web Browser	The Science User populates forms with ECS registration information. This information includes: user name, address, telephone number, email address, and user verification key (for security confirmation). The user then submits this information.
A.2.1	Submit User Registration Request	EcClDtUserProfileGateway	EcMsAcRegUserSrvr	Distributed Object	The User Registration Tool submits the User Registration Request to the User Registration Server for approval.
A.2.2	Store a User Registration Request	EcMsAcRegUserSrvr	Sybase	CtLib	The User Registration Request is saved for approval by DAAC User Services.
A.3.1	Startup User Registration Server GUI	DAAC Ops - User Services	EcMsAcRegUserGUI	Xterm	DAAC operations remotely start the SMC User Registration Server GUI after logging into the SMC.
A.3.2	Review New User Request	DAAC Ops - User Services	EcMsAcRegUserGUI	Xterm	On a periodic basis (based on DAAC policy), User Services checks for any new User Registration Requests.
A.3.3	Get New User Requests	EcMsAcRegUserGUI	EcMsAcRegUserSrvr	Distributed Object	Request all new User Registration Requests. The GUI connects to the Registration Server at the SMC.
A.3.4	Retrieve User Registration Requests	EcMsAcRegUserSrvr	Sybase	CtLib	All pending User Registration Requests for the operator’s home DAAC are retrieved from the database.
A.4.1	Update User Request	EcMsAcRegUserGUI	EcMsAcRegUserSrvr	Distributed Object	DAAC User Services completes the User Profile from the request. Updated information includes V0Gateway User name, group and password.

Table 4.16.2.2-1. Component Interaction Table: User Registration (2 of 2)

Step	Event	Interface Client	Interface Provider	Interface Mech	Description
A.4.2	Create User Profile	EcMsAcRegUserGUI	EcMsAcRegUserGUI	Distributed Object	User Registration Server takes the completed User Registration Request and makes a User Profile, registering the user.
A.4.3	Store a User Profile	EcMsAcRegUserSrvr	Sybase	CtLib	The User Profile is saved in the SMC User Profile Database.
A.5.1	Send E-mail	EcMsAcRegUserSrvr	CsEmMailRelA (to Science User)	e-mail	A Confirmation message is sent to the new ECS Science User, via CSS infrastructure mail services (CsEmMailRelA).
A.7.1	Replicate User Profile	Sybase	Sybase	EcMsRsDb	The user profile is replicated at each DAAC via the Sybase Replication Server.

4.17 Sybase Replication Server

The concept of a domain is useful when describing a replication system. Briefly, a domain is a set of replication servers and their associated components that communicate with each other. A domain can be one replication server that replicates data from a local primary database to another local replicate database (as in a warm standby application) or a domain can contain many replication servers distributed over a wide area network (WAN) as will be the case for the MSS.

Each domain requires one, and only one, ID server. An ID server is a replication server that is specified as such when it is installed. An ID Server assigns unique identifiers to domain components. The ID server must be the first replication server installed in a domain and must be accessible when any component is added to the domain.

When a replication server is installed (including the ID Server), the following components are created:

- A database called the Replication Server System Database (RSSD) (the data server housing the RSSD must already exist)
- A stable device (queue)
- An interface (connection) to the RSSD data server
- A RepAgent for the RSSD

The RSSD contains system tables that are used by the replication server. In a mutli-server domain that implements consolidated distributed primary fragments, the RSSDs must also be replicated. The RSSD contains information about each domain component, component login ids and passwords, application specific objects such as replication definitions, replicate transaction identifiers, routes and connections, and replicate transaction errors.

The RSSD data model is documented in the manual *Replication Server Reference Manual*.

As additional replication servers are added to a domain, the replication system administrator creates replication server interfaces (RSI), or routes, between the replication servers. Routes allow replicate transactions to “flow” from a primary replication server to a replicate replication server.

Finally, application databases are added to a domain. For each database added to the domain the following components are created:

- For primary databases, an log transfer manager (LTM), which transfers database transactions from the primary database to the replication server
- For replicate database an interface from the replicate replication server to the replicate database

4.18 Replication System Administrator (RSA)

Administering the replication system is primary the role of the Replication System Administrator (RSA). The Replication System Administrator installs, configures, and administers the replication system. Given the distributed nature of the MSS implementation this role may be performed by different people at different locations. If this is the case, various tasks for administering Replication Server may require coordination between Replication System Administrators.

The Replication System Administrator has sa user permissions, which provides that person with the ability to execute nearly all commands in the replication system. In managing the system, the Replication System Administrator may need to coordinate with DBAs for both local and remote databases.

Replication System Administrators should be experienced Sybase DBAs and should have taken the Sybase training classes Replication System Administration and Replication Disaster Recovery Workshop. They should also have read and understood the manuals: *Replication Server Administration Guide*, *Replication Server Configuration Guide for UNIX Platforms*, *Replication Server Reference Manual*, and *Replication Trouble Shooting Guide*.

4.18.1 Replication System Administrator Tasks

The tasks shown in Table 4.18.1-1 are required to maintain a replication system:

Table 4.18.1-1. Replication System Administrator Tasks

Task	Roles
Installing Replication Server	Replication System Administrator (RSA)
Adding or removing a Replication Server	RSA
Starting up and shutting down Replication Server.	RSA
Configuring Replication Server	RSA
Maintaining Routes (Creating and modifying)	RSA
Managing the RSSD	RSA
Adding a primary and replicate database.	RSA
Adding login names, database users, and administering appropriate permissions	RSA
Adding replicated tables or changing table schemas. Creating and modifying replicated tables Creating and modifying replication definitions Creating and materializing subscriptions at replicate sites.	RSA
Defining data server function-string classes and function strings.	RSA
Applying database recovery procedures.	RSA
Maintaining and monitoring database connections	RSA
Monitoring Replication Server	RSA
Perform Database Rebuilds	RSA
Perform Database Patches	RSA
Processing rejected transactions	RSA
Quiescing Replication Server	RSA
Reconciling database inconsistencies.	RSA

4.18.2 DAAC DBA Replication Roles and Tasks

The Database Administrator (DBA) plays a subsidiary role by supporting some Replication Server administrator task. Table 4.18.2-1 shows tasks that the DBA administrators perform at the local DAACs with respect to replication server administration.

Table 4.18.2-1. DAAC DBA Replication Roles and Tasks

Task	Roles
Installing Replication Server	Database Administrator (DBA)
Managing the RSSD	DBA
Adding a primary and replicate database.	DBA
Perform Database Rebuilds	DBA
Perform Database Patches	DBA
Adding login names, database users, and administering appropriate permissions	DBA
Adding replicated tables or changing table schemas. Creating and modifying replicated tables Creating and modifying replication definitions Creating and materializing subscriptions at replicate sites.	DBA
Defining data server function-string classes and function strings.	DBA
Applying database recovery procedures.	DBA
Processing rejected transactions	DBA
Quiescing Replication Server	DBA
Reconciling database inconsistencies.	DBA

4.19 Sybase Replication Server Installation and Setup

4.19.1 Sybase Replication Server 11.5.1

The Sybase Replication server software that will be delivered to the DAACs must be installed on the MSS primary machines. Other than copying the software to the directories specified in the PSR, no further action for configuring the COTS product is necessary. This installation makes the rs_subcmp utility available to the CUSTOM scripts.

4.19.2 Custom Installation

The replication package must be installed onto the appropriate mode/machines. Instructions will be delivered with the software drop.

The following software will need to be run:

- MSS db patch
- rs_UsrInstall

4.19.2.1 MSS database patch

Since replication will only occur between tables sharing the same schema, the MSS must be run for replication to occur successfully. The database patches will add the Sybase login mss_acct_db_maint for replication to/from the SMC in addition to bringing the database into compliance with database schema requirements.

4.19.2.2 rs_UsrInstall script

The rs_UsrInstall script will need to be configured and executed at each site. Instructions will be delivered with the software drop. The DAAC installers will need to coordinate with the SMC as to setting password, servername, and database name parameters for the replication script. This script creates the script rs_UsrMain and its associated files based are the parameters entered by the installer.

The rs_UsrMain script is the script that will need to be run for replication to occur with the SMC.

Lastly, email addresses for the replication administrators (i.e. staff who need to be notified of error conditions) will need to be added to the email notification file located in the …/CUSTOM/dbms/COM/DBAdmin directory.

4.20 Other Installation

The Sybase administrator will need to update the Sybase Interfaces files on the MSS primary servers.

4.20.1 Sybase Replication for Subsequent Database Builds

4.20.1.1 Build Process

1) If Sybase replication already exists in the database mode. The replication subscriptions at the replicated site must be dropped, then the replication definition at the primary site must be dropped prior to running the build script.
2) The table schema must be the same at the primary and replicated sites for the tables that will be contain replicated data.

4.20.1.2 Database Access

1) The "sa" user passwords must be the same on the replication servers and SQL Servers at the primary and replicated sites prior to subscribing to the replicated data.
2) The maintenance user must exist in the primary and replicated databases and have grant all permissions on the replicated tables. The maintenance user should have been added during the database build process.
3) All other sybase logins, database users and database permissions must have created successfully.

4.20.1.3 Enabling Sybase Replication

4.20.1.3.1 Preconditions:

- The direct routes between the replication servers included in the replication system must be up.
- The RepAgent and Database Server Interface (DSI) threads must be up for the Replication Server System Databases (RSSD) included in the replication system.
- The database that will contain replicated data must be known to the replication system.
- The RepAgent and DSI threads must be up for the databases included in the replication system.

4.20.1.3.2 Customized Scripts to Support Replication:

1) The customized scripts to install replication components must be run successfully.
2) Reference the Sybase Replication Installation and Configuration instructions that were delivered with the software drop.

4.20.2 Sybase Replication for Database Patches

4.20.2.1 Patch Process

1) If the table schema at the primary site for the replicated data will be changed during the patch process. The replication subscriptions at the replicated site must be dropped, then the replication definition at the primary site must be dropped prior to running the patch script.
2) The database patch script must be run successfully for the primary and replicated databases.
3) The table schema must be the same at the primary and replicated site for the tables that will be contain replicated data.

4.20.2.2 Database Access

1) at the primary and replicated sites prior to subscribing to the replicated data.
2) The "sa" user passwords must be the same on the replication servers and SQL Servers The maintenance user must exist in the primary and replicated databases and have grant all permissions on the replicated tables. The maintenance user should have been added during the database build process.
3) All other sybase logins, database users and database permissions must have created successfully.

4.20.2.3 Enabling Sybase Replication

4.20.2.3.1 Preconditions:

- The direct routes between the replication servers included in the replication must be up.
- The RepAgent and Database Server Interface (DSI) threads must be up for the Replication Server System Databases (RSSD) included in the replication system.
- The database that will contain replicated data must be known to the replication system.
- The RepAgent and DSI threads must be up for the databases included in the replication system.

4.20.2.3.2 Customized Scripts to Support Replication:

1) If the replication definition was modified to support a table schema change, then the script to install the revised replication definition must be run at the primary site. After the replication definition has been installed successfully, then the script to install the replication subscription must be run at the replicated site.
2) Reference the Sybase Replication Installation and Configuration instructions that were delivered with the software drop. Any function string class and error class that were installed as part of replication will NOT have to be reinstalled.

4.21 Error Conditions

The output of the rs_subcmp utility is logged to EcMsRepSubCmp.log in the …/CUSTOM/logs directory. If an error condition is detected (by grepping the log after completion of the script) an email is sent to the addresses listed in the email notification file.

4.22 DAAC/SMC Coordination Issues

The DAACs should coordinate the following issues with the SMC and vice/versa.

- MSS Database Schema Versions
- Changes to the Sybase password for login mss_acct_db_maint

4.22.1 MSS Database Schema Version

When the SMC or a DAAC executes a database patch that changes the MSS User Profile table schema, the rs_UsrMain script will prevent execution of the rs_subcmp utility and this condition will be logged and email notification will be sent. Database patches to the MSS database should be coordinate through the SMC.

4.22.2 MSS Login Maintenance

If the password of the mss_acct_db_maint login is changed at the SMC, then the configuration files associated with rs_UsrMain will need to be updated at the SMC and at the DAACs to reflect the change.

If a DAAC changes the password of the user id, then that DAAC and SMC will need to update the configuration files associated with the rs_UsrMain script.

4.23 Replication Administration Software

Some of the Replication Server administration tasks will be supported by COTS and/or custom software (scripts). The COTS consists of the Sybase products Replication Server Manager (RSM) and Sybase Central, a GUI based administration tool.

Scripts will be developed for the following administration tasks in support of installing and configuring Replication Server and for installing replication server objects that are specific to the MSS application.

- Creating Routes
- Managing the RSSD
- Adding login names, database users, and permissions
- Creation of replication definitions, subscriptions, function strings and error classes
- Subscription materialization

4.23.1 Monitoring

The Sybase Central/RSM products will be used for the following tasks:

- Configuring Replication Server
- Modifying Routes
- Maintaining and monitoring database connections
- Monitoring Replication Server

Scripts that will be executed by the RSM will be developed to notify the RSA of the following events:

Component	*Event*
Servers	Active, Quiesed, Suspect, Hung, Shutdown, Dead, Unknown, Invalid
Routes	Change in status
Connection	Change in status
Partition	State change, size threshold exceeded
Queues	Latency threshold exceeded, size threshold exceeded
Database	Latency threshold exceeded

4.24 Recovery

Scripts will be developed to restore the RSSD or to bring application databases to a consistent state.

RSSD Recovery

- dumpdb
- dumptran
- logsegment threshold
- data segment threshold

MSS Database Recovery

- last chance logsegment threshold modification to disable secondary truncation point
- rs_subcmp scripts for each subscription in the domain

Sybase Central/RSM will be used for the following recovery tasks:

- Processing Rejected Transactions
- Quiesing Replication Server

4.25 Network and Security Requirements

The Sybase interface files used by the Replication Servers at each DAAC will need to be modified to locate all Sybase Replication and Data Server in the replication domain. Additionally, subscription materialization requires the same user id and password for the replicate replication server and the primary and replicate data servers. Replication server userid and password maintenance must be coordinate across sites. Replication server supports password encryption, and this feature will.

4.26 A DAAC is Added to the Replication Domain

EROS DATA Center (EDC) is added to the domain, which before its installation includes, GSF, LAR, and NSC.

Task	Role	Site
The replication server software is copied to the local host.	RSA	EDC
Replication servers and MSS SQL servers are added to the interfaces files	RSA, DBA	All
The replication server executable, and its RSSD is created.	RSA, DBA	EDC
create route SMCF to EDC	RSA	EDC
The routes are verified at each site by executing the rs_helproute command on each DAAC's RSSD ASE server.	RSA	All
The rs_init utility is executed to add EDC's mss_acct_db to the operational domain. The utility connects to the ID server at SMC to obtain unique id information for the database. The rs_init utility creates an LTM start file and starts the LTM.	RSA	EDC
Create replication definition MsAcUsrProfile	RSA	EDC
Create replication definition EcAcRequest	RSA	EDC
Create, verify, and materialized subscription MsAcUsrProfile_SMC_EDC	RSA	EDC

4.27 Fault Recovery Scenarios

4.27.1 General Faults

In general, Sybase Replication Server is fault tolerant. Replicate database transactions start in the primary database's transaction log, are transferred from the log to the primary replication server's queue, then to the replicate replication server's queue before being applied to the replicate databases. Database transactions are not removed from a log or a queue until the transaction has successfully moved to its next destination.

During temporary system faults, the transaction remains in its log or queue, until the fault is recovered. For example, if the replicate Sybase Server at NSC is shutdown for maintenance, replicate transactions from other DAACs are stored in the NSC's stable queue until the Sybase Server is brought back online. When NSC's replication server re-establishes its connection to the Sybase Server, the queued transactions will be applied to the replicate database in the order received. This approach is followed for all component failures.

When a failure occurs for an extended period or is of the type that causes a loss of replicate transactions (e.g. the failure of a devices supporting a queue or log), additional recovery steps must occur between sites.

4.27.2 EDC Experiences an LTM failure

The transaction log of the mss_acct_db at EDC is half full when the EDC's LTM suddenly, and expectedly, crashes. Meanwhile, a large number of orders are requested and the database's transaction log reaches its last-chance threshold. The threshold-stored procedure fires and forces a truncation of the transaction log. The stored procedure will log an error message in the SQL Server error log to serve notice that the truncated transactions have not been replicated. The threshold-stored procedure prevents the mss_acct_db database from 'freezing'; however, a recovery procedure will need to be used to forward the lost transactions to other DAACs.

The following tasks must occur:

Task	Role	Site
All client connections to the EDC SQL Server are suspended. Any transaction coming into EDC from other DAACs is queued in the EDC replication server stable device.	RSA, DBA	EDC
The EDC Replication Server's stable device is cleared of any open transactions.	RSA	EDC
The EDC mss_acct_db transaction log is dumped.	DBA	EDC
After verifying that EDC's transactions in the GSF stable queue have been processed, the rs_subcmp utility is executed to update EDC's primary fragment at GSF.	RSA	GSF
After verifying that EDC's transactions in the LAR stable queue have been processed, the rs_subcmp utility is executed to update EDC's primary fragment at LAR.	RSA	LAR
After verifying that EDC's transactions in the NSC stable queue have been processed, the rs_subcmp utility is executed to update EDC's primary fragment at NSC.	RSA	NSC
The LTM at EDC is started.	RSA	EDC
Set the secondary truncation point at EDC to valid.	DBA	EDC
Resume client application connections to the EDC SQL Server.	DBA, RSA	EDC
Resume the DSI connection at EDC.	RSA	EDC

4.27.3 The GSF MSS Database Becomes Corrupt and Needs to be Restored from Backup

The GSF mss_acct_db database was dumped at 12:00am. A database transaction dump executed successfully at 8:00 am. At 12:00pm, GSF's database logs become corrupt and the SQL server takes the database off-line and suspends client connections using the database.

Task	Role	Site
The LTM is shutdown.	RSA	GSF
Restart the GSF Replication Server in standalone mode.	RSA	GSF
The command admin get_generation, data_server, database is executed on the GSF Replication Server.	RSA, DBA	GSF
The command set log recovery for data_server.database is executed.	RSA	GSF
A checkpoint is issued in the mss_acct_db database.	DBA	GSF

(Cont'd)

Task	Role	Site
The GSF LTM is started with the for_recovery option.	RSA	GSF
The 12:00 am database dump and the 8:00am transaction dump are loaded.	DBA	GSF
The GSF LTM is shutdown.	RSA	GSF
The command rs_zeroltm, e0mss20_srvr, mss_acct_db is executed.	RSA	GSF
The command dbcc settrunc('ltm', 'gen_id', <new_number>) is executed.	DBA	GSF
The rs_subcmp utility is executed to synchronize EDC's copy of GSF's user profile primary fragment.	RSA	EDC
The rs_subcmp utility is executed to synchronization EDC's copy of GSF's EcAcRequest primary fragment.	RSA	EDC
The rs_subcmp utility is executed to synchronize LAR's copy of GSF's user profile primary fragment.	RSA	LAR
The rs_subcmp utility is executed to synchronize NSC's copy of GSF's user profile primary fragment.	RSA	NSC
Restart the GSF Replication Server in normal mode.	RSA	GSF
The LTM is started	RSA	GSF
Connections are resumed at the GSF SQL Server	DBA	GSF

4.27.4 EDC RSSD Becomes Corrupt and Needs to be Restored

RSSD recovery is different depending on the activity that occurred since the RSSD was dumped. There are four increasingly severe levels of RSSD failure with increasingly complex recovery requirements.

Activity Since Last RSSD Dump	Procedure
No DDL activity	Basic RSSD Recovery Procedure
DDL activity, but no new routes or subscriptions created	Subscription Comparison Procedure
DDL activity, no new routes created	Subscription Re-Creation Procedure
New routes created	Deintegration/Reintegration Procedure (involves removing and reinstalling replication server)

This scenario assumes that no Data Definition Language (DDL) activity occurred since the last RSSD dump. DDL commands in replication command language (RCL) include those for creating, altering, or deleting routes, replication definitions, subscriptions, function strings, functions, function-string classes, or error classes.

Tasks for Basic RSSD Recovery Procedure:

Task	Role	Site
Shutdown all RepAgents and LTM that connect to the Replication Server.	RSA	EDC
Shutdown the Replication Server if it is not down.	RSA	EDC
Restore the RSSD by loading the most recent RSSD database dump and transaction dumps.	RSA, DBA	EDC
Restart the Replication Server in standalone mode.	RSA	EDC

(Cont’d)

Task	Role	Site
Log into the Replication Server and get the generation number for the RSSD.	RSA	EDC
Rebuild the Replication Server queues.	RSA	EDC
Start all RepAgents and LTMs in recovery mode.	RSA	EDC
Check the loss messages in the Replication Server log, and in the logs of all Replication Servers with direct routes from the current Replication Server. (GSF, LAR, NSC) If a loss is detected, see the recovery procedure for scenario The GSF MSS database may have become corrupt and may need to be restored from backup.	RSA	All
Shutdown the LTM managed by the current Replication Server.	RSA	EDC
Execute the dbcc settrunc command at the Adaptive Server for the restored RSSD. Move up the secondary truncation point.	RSA, DBA	EDC
Execute the dbcc settrunc command at the Adaptive Server for the restored RSSD to set the generation number to one higher than the number returned in step 5.	RSA, DBA	EDC
Restart the Replication Server in normal mode.	RSA	EDC
Restart the RepAgents for the RSSD and the LTM in normal mode.	RSA	EDC

ASF is now part of replication domain.

4.28 Reference Documents

The following are reference documents and other information that will be helpful in the administration of Sybase Replication Server.

Name	Web site Address
Sybase Web Site	http://www.sybase.com/
Points of Contact web site Address	http://m0mss01.ecs.nasa.gov/smc/
Replication Server Reference Manual	http://www.sybase.com/products/datamove/
Sybase Central Installation Instruction	http://cmdm.east.hitc.com
Replication Server Manager Installation Instruction	http://cmdm.east.hitc.com
609-EMD-001, Release 7 Operations Tools Manual	http://edhs1.gsfc.nasa.gov/waisdata/catalog/
Database Administrators	http://www.sybase.com
Configuration Parameter Document	http://cmdm.east.hitc.com
DBA/RSA Points of Contact at web site Address	http://m0mss01.ecs.nasa.gov/smc/
313-EMD-001, Release 7 ECS Internal Interface Control Document for the EMD Project	http://edhs1.gsfc.nasa.gov/waisdata/catalog/
625-EMD-013, Training Material for the EMD Project, Volume 13: User Services	http://edhs1.gsfc.nasa.gov/waisdata/catalog/

5. Security Services

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. Security logs are monitored and security reports generated by the System Administrator as required. Several open source products provide tools for authentication and network and systems monitoring - Crack, ANLpasswd, TCP Wrappers, and Tripwire. Crack and ANLpasswd provide brute force password cracking and password checking, respectively for local system and network access. Tripwire monitors for intruders by noting changes to files. F-Secure Secure Shell (ssh) provides strong authentication access and session encryption for ECS from external, non-trusted networks as well as internally within a DAAC. Security Services also supports detection of, reporting, and recovery from security breaches. Security scans of each system are performed periodically to prepare for the formal security scans done biannually by the ESDIS IV&V contractor. These preliminary scans are done using the ISS Internet Security Scanner product.

The following section defines step-by-step procedures for Operations personnel to run the Security Services tools. These procedures assume that DAAC Management has already approved the requester's application for a Security process. It is recommended that access to these tools be controlled through the **root access only**.

5.1 Scanning Network Vulnerabilities

ECS is no longer responsible for scanning the network and network-attached systems. However, the ISS Internet Security Scanner is a licensed product that NASA uses extensively to detect system level vulnerabilities. GSFC has a site license to use the product and any ECS DAAC may use that license since all DAACs are using GSFC IP address space. This product does NOT belong to ECS and as such there is not an official release of it. A license key is required which can be obtained from the ESDIS Computer Security Official, who is currently Clayton Sigman (Clayton.Sigman@gsfc.nasa.gov). The information he will need is the IP addresses of the Production and M&O LANs. The software runs on Microsoft Windows NT or Microsoft Windows 2000. A laptop is the only practical way to run it. Once you have the key, the product is downloadable from:

http://www.iss.net/download

You must register in order to get an account and password to download the product. The setup is like most PC products – run the setup.exe that you downloaded. It will query you for the license key.

ISS uses profiles, which tailor what and how it queries systems. To get the most recent version, contact the IV&V contractor, Titan Inc. at 301/982-5414 and ask for the ESDIS security group.

5.2 Ensuring Password Integrity

One aspect of system security is discretionary access control based on user passwords. Passwords ideally would be so unique that they are virtually impenetrable to unauthorized users. Two products provide utilities to create effective password practices. "Crack" detects weak passwords that could be easily bypassed. It works in "batch" mode. ANLpasswd enforces strong password rules as the user is changing their password.

Crack and ANLpasswd provide a comprehensive dictionary, which can be shared. These "source" dictionaries provide lists of words, which if used, would create vulnerable passwords. You can add other dictionaries, for example, acronym lists, to eliminate commonly used terms from being used as passwords.

Crack is installed in a secure location that has **root access only**. ANLpasswd is automounted in /tools/bin.

5.2.1 Detecting Weak Passwords

Running Crack against a system's password file enables a system administrator to assess how vulnerable the file is to unauthorized users and how well authorized users select secure passwords. Crack is designed to find standard Unix eight-character DES-encrypted passwords by standard guessing techniques.

Crack takes as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary or from information gleaned about users from the password file. It does not attempt to remedy the problem of allowing users to have guessable passwords, and it should NOT be used in place of getting a really good, secure password program replacement.

The instructions provided in the following sections are general in nature, because how you configure Crack is DAAC specific. Operations personnel should be familiar with these tasks to:

- Configure the Crack shell script and config.h files based on the README file and on requirements established for your site. See the Section on “Configuring Crack” below.
- Run Crack based on requirements established for your site. See “Running Crack” below.
- Customize the dictionaries. See Section “Creating Dictionaries” below.

5.2.1.1 Configuring Crack

Although Crack should already be configured for your system, the instructions are provided should you have to reconstruct the makefile as a result of file corruption. Crack has two configuration files: the Crack shell script, which contains all the installation-specific configuration data, and the file Sources/conf.h, which contains configuration options specific to various binary platforms. Use the following procedure for configuring crack.

1 In the Crack shell script, edit the CRACK_HOME variable to the correct value. This variable should be set to an absolute path name on which Crack will be run. (Path names relative to username are acceptable as long as you are using csh.)

- There is a similar variable, CRACK_OUT, which specifies where Crack should put its output files — by default, this is the same as $CRACK_HOME.

2 Edit the file Sources/conf.h and establish which switches to enable. Each #define has a small note explaining its purpose. Portability of certain library functions, should not be a problem.

3 If using Crack-network (see Section 5.2.1.4, Options, below), generate a Scripts/network.conf file. This file contains:

- a list of hostnames that are rsh/ssh destinations.
- their binary type (useful when running a network Crack on several different architectures).
- an estimate of their relative power (take your slowest machine as unary, and measure all others relative to it).
- a list of per-host flags to add to those specified on the Crack command line, when calling that host.
- There is an example of such a file provided in the Scripts directory.

4 To specify a more precise figure as to the relative power of your machines, play with the command *make* tests in the source code directory. This can provide you with the number of fcrypt()s that your machine can do per second. This number can be plugged into your *network.conf* as a measure of your machines' power (after rounding the value to an integer).

5.2.1.2 Running Crack

Crack is a self-installing program. Once the necessary configuration options for the Crack shell script and config.h have been set, the executables are created via *make* by running the Crack shell script.

NOTE: To run Crack on a YP password file, the simplest way is to generate a passwd format file by running:-

# ypcat passwd > passwd.yp ↵

and then running Crack on the passwd.yp file.

To launch Crack:

1 To change directory, type **cd /usr/local/solaris /crack**, and then press the **Return/Enter** key.

2 To execute the program, type **./Crack**, and then press the **Return/Enter** key.

3 For the single platform version, type **./Crack [options] [bindir] /etc/passwd [...other passwd files]** , and then press the **Return/Enter** key.

4 To execute over the network, type **./Crack -network [options] /etc/passwd [...other passwd files]** , and then press the **Return/Enter** key.

For a brief overview of the [options] available, see Section 5.2.1.4, Options, below. Section 5.2.1.5, Crack Support Scripts, briefly describes several very useful scripts.

5.2.1.3 Creating Dictionaries

Crack works by performing several individual passes over the password entries that are supplied. Each pass generates password guesses based upon a sequence of rules, supplied to the program by the user. The rules are specified in a simplistic language in the files gecos.rules and dicts.rules, located in the Scripts directory (see Section 5.2.1.5, Crack Support Scripts, below).

Rules in Scripts/gecos.rules are applied to data generated by Crack from the pw_gecos and pw_gecos entries of the user's password entry. The entire set of rules in gecos.rules is applied to each of these words, which creates many more permutations and combinations, all of which are tested. After a pass has been made over the data based on gecos information, Crack makes further passes over the password data using successive rules from the Scripts/dicts.rules by loading the whole of Dicts/bigdict file into memory, with the rule being applied to each word from that file. This generates a resident dictionary, which is sorted and made unique to prevent wasting time on repetition. After each pass is completed, the memory used by the resident dictionary is freed up, and re-used when the next dictionary is loaded.

Crack creates the Dicts/bigdict dictionary by merging, sorting, and making unique the source dictionaries, which are to be found in the directory DictSrc and which may also be named in the Crack shell script, via the $STDDICT variable. (The default value of $STDDICT is /usr/dict/words.)

The file DictSrc/bad_pws.dat is a dictionary that is meant to provide many of those common but non-dictionary passwords, such as 12345678 or qwerty.

To create your own dictionary:

1 Copy your dictionary into the DictSrc directory (use compress on it if you wish to save space; Crack will unpack it while generating the big dictionary).

2 Delete the contents of the Dicts directory by running Scripts/spotless. Your new dictionary will be merged in on the next run.

5.2.1.4 Options

Options available with the Crack command are:

-f Runs Crack in foreground mode, i.e., the password cracker is not put into the background, and messages appear on stdout and stderr as you would expect. This option is only really useful for very small password files, or when you want to put a wrapper script around Crack.

Foreground mode is disabled if you try running Crack-network -f on the command line, because of the insensibility of rsh'ing to several machines in turn, waiting for each one to finish before calling the next. For more information, read the section about Network Cracking without NFS/RFS in the README.NETWORK file.

-v Sets verbose mode, whereby Crack will print every guess it is trying on a per-user basis. This is a very quick way of flooding your filestore, but useful if you think something is going wrong.

-m Sends mail to any user whose password you crack by invoking Scripts/nastygram with their username as an argument. The reason for using the script is so that a degree of flexibility in the format of the mail message is supplied; i.e., you don't have to recompile code in order to change the message.

-nvalue Sets the process to be nice()ed to value, so, for example, the switch -n19 sets the Crack process to run at the lowest priority.

-network Throws Crack into network mode, in which it reads the Scripts/network.conf file, splits its input into chunks which are sized according to the power of the target machine, and calls rsh to run Crack on that machine. Options for Crack running on the target machine may be supplied on the command line (for example, verbose or recover mode), or in the network.conf file if they pertain to specific hosts (e.g., nice() values).

-r<pointfile>

This is only for use when running in recover mode. When a running Crack instance starts pass 2, it periodically saves its state in a point file, with a name of the form Runtime/P.* This file can be used to recover where you were should a host crash. Simply invoke Crack in exactly the same manner as the last time, with the addition of the **-r** switch (for example, **-rRuntime/Pfred12345**). Crack will startup and read the file, and jump to roughly where it left off. If you are cracking a very large password file, this can save a lot of time after a crash.

5.2.1.5 Crack Support Scripts

The Scripts directory contains a small number of support and utility scripts, some of which are designed to help Crack users check their progress. The most useful scripts are briefly described below.

Scripts/shadmrg

This is a small script for merging /etc/passwd and /etc/shadow on System V style shadow password systems. It produces the merged data to stdout, and will need to be redirected into a file before Crack can work on it.

Scripts/plaster

This is a simple front-end to the Runtime/D* diefiles that each copy of the password cracker generates. Invoking Scripts/plaster will kill off all copies of the password cracker you are running, over the network or otherwise. Diefiles contain debugging information about the job, and are generated so that all the jobs on the entire network can be called quickly by invoking Scripts/plaster. Diefiles delete themselves after they have been run.

Scripts/status

This script rsh's to each machine mentioned in the Scripts/network.conf file, and provides some information about processes and uptime on that machine. This is useful when you want to find out just how well your password crackers are getting on during a Crack -network.

Scripts/{clean,spotless}

These are just front ends to a makefile. Invoking Scripts/clean cleans up the Crack home directory and removes unwanted files, but leaves the pre-processed dictionary bigdict intact. Scripts/spotless does the same as Scripts/clean, but obliterates bigdict and old output files, too, and compresses the feedback files into one.

Scripts/nastygram

This is the shell script that is invoked by the password cracker to send mail to users who have guessable passwords, if the **-m** option is used. Edit it to suit your system.

Scripts/guess2fbk

This script takes your out* files as arguments and reformats the 'Guessed' lines into a feedback file, suitable for storing with the others.

An occasion where this might be useful is when your cracker has guessed a large number of passwords and then died for some reason (a crash?), before writing out the guesses to a feedback file. Running **Scripts/guess2fbk out* >> Runtime/F.new** will save the work that has been done.

5.2.1.6 Checking the Log

Crack loads dictionaries directly into memory, sorts and makes them unique, before attempting to use each of the words as a guess for each users' password. If Crack correctly guesses a password, it marks the user as done and does not waste further time on trying to break that user's password.

Once Crack has finished a dictionary pass, it sweeps the list of users looking for the passwords it has cracked. It stores the cracked passwords in both plain text and encrypted forms in a feedback file in the directory **Runtime**. Feedback files have names of the form **Runtime/F***. This allows Crack to recognize passwords that it has successfully cracked previously, and filter them from the input to the password cracker. This provides an instant list of “crackable” users who have not changed their passwords since the last time Crack was run. This list appears in a file with name **out*** in the **$CRACK_OUT** directory, or on **stdout**, if foreground mode (**-f**) is invoked (see Section “Options”, above).

Similarly, when a Crack run terminates normally, it writes out to the feedback file all encrypted passwords that it has NOT succeeded in cracking. Crack will then ignore all of these passwords next time you run it.

Obviously, this is not desirable if you frequently change your dictionaries or rules, so, **Scripts/mrgfbk** is provided to allow for checking the “uncrackable” passwords. This script sorts your feedback files, merges them into one, and optionally removes all traces of "uncrackable" passwords, so that your next Crack run can have a go at passwords it has not succeeded in breaking before.

mrgfbk is invoked automatically if you run **Scripts/spotless** (see Section 5.2.1.5, Crack Support Scripts, above).

5.2.2 Configuring ANLpasswd

The Argonne National Laboratory wrote ANLpasswd and has made it available to everyone as freeware. There is a simple install script that will install the components on the automount host for both SGI and Sun architectures. ANLpasswd consists of a setuid C program that is used to call the anlpasswd Perl script. The Perl script uses the Crypt:: Cracklib module, which is installed with the package, a dictionary generation tool, and dictionaries that are used to match attempted passwords against possible passwords that are in the dictionary file.

It is assumed that Perl 5.6 is properly installed in /tools/perl for Sun and SGI platforms. The binary ypstuff and the anlpasswd30 script (with its soft links to anlpasswd and yppasswd) are placed in /tools/bin. The Perl includes and dictionary file should also be NFS mounted and placed in /tools/lib/anlpasswd.

Once the package is configured, the only alteration may be in the dictionary files. There are a large number of dictionary files that are included by default in this release. If there are local requirements to change them (i.e. the default has too little security or too much security), the following procedure is applicable.

1 Login to the automount host as root or **su** to root.

2 Modify the SGI /tools/lib/words directory as required (add files, modify files or remove files).

3 Remove the Sun /tools/lib/words directory contents, then copy the SGI (modified) directory to the Sun directory.

4 Login to an SGI as root or **su** to root.

5 From the SGI window, type **cd /tmp** and then press the **Return/Enter** key to change to the directory where anlpasswd-30.tar.gz is located.
- The directory is changed to **/tmp**.

6 To explode anlpasswd-30.tar.gz, type **gzip –dc anlpasswd-30.tar.gz | tar –xovf –** and ten press the **Return/Enter** key.
- The anlpasswd-30.tar.gz file is exploded.

7 From the SGI window, to change directory to the location of the make dictionary script, type **cd /tmp/anlpasswd/anlpasswd-3.0-sgi/cracklib25_small**, and then press the **Return/Enter** key.
- The directory is changed to /tmp/anlpasswd/anlpasswd-3.0-sgi/cracklib25_small.

8 To run the make dictionary script, type **./makedictionary.pl** and then press the **Return/Enter** key.
- ***Note*:** perl expected to be in /tools/perl
- The script runs.

9 From the SGI window, on completion, copy the pw_dict.* files to the automount host's /tmp directory.

10 From the automount host window, copy the /tmp/pw_dict.* files to the appropriate /tools/lib directories for ***both*** SGI and Sun architectures.

11 Logout from the automount host.

12 From the SGI window, **su** to a normal user account and check that the changes work by running /tools/bin/anlpasswd as a normal user and verify at least one of the changes and that the script still works normally (without errors).

13 From the SGI window, to delete the temp files, type **rm –rf /tmp/anlpasswd**, and then press the **Return/Enter** key.
- The temp files are deleted.

14 Logout from the SGI.

5.2.2.1 Installing ANLpasswd

1 Copy the anlpasswd-30.tar.gz file to a staging area.
- ***Note*****:** For convenience, **/tmp** is used in these instructions.

2 Login to the automount host as root or **su** to root.

3 To change directory to /tmp, type **cd /tmp** and then press the **Return/Enter** key.
- The directory is changed to /tmp.

4 To explode the tarball, type **gzip –dc anlpasswd30.tar.gz | tar –xovf –** and then press the **Return/Enter** key.
- The file is exploded.

5 To change to the top level directory, type **cd /tmp/anlpasswd** and then press the **Return/Enter** key.
- The directory is changed to /tmp/anlpasswd.

6 To run the install script, type **./install_anlpasswd.pl** and then press the **Return/Enter** key.
- The script runs, installing the **/tools/bin/anlpaswd30** script with links to **/tools/bin/anlpasswd**, **/tools/bin/yppasswd**, the dictionaries themselves, and the dictionary indexes.

The next task is to change passwords.

1 Checkout the SGI installation from an SGI production host by logging in as a normal user.

2 To change your password, type **/tools/bin/yppasswd**, and then press the **Return/Enter** key.
- Follow the on-screen prompts to complete entry of the current password and then entry and confirmation of the new password.

3 Logout.
- Wait a few minutes to make sure that the updates are completed.

4 Checkout the Solaris installation from a Sun production host by logging in as a normal user.

5 To change your password, type **/tools/bin/yppasswd**, and then press the **Return/Enter** key.
- Follow the on-screen prompts to complete entry of the current password and then entry and confirmation of the new password.

6 Logout

- Wait a few minutes to make sure that the updates are completed.

5.2.2.2 ANLpasswd readme

The following is the README.INSTALL from the tar file with comments. This work has already been incorporated in the release. It is provided here to facilitate understanding of how the product is put together.

```
ANLpasswd is used in ECS to provide interactive password checking. It is
installed on the network in the /tools/bin directory. Local installation
is not required.

PREREQUISITES
This installation requires:
Perl 5.6.1
50Mb of disk space
It will take approximately 30 minutes to complete this installation.

INSTALLATION INSTRUCTIONS
1.  Copy the anlpasswd-30.tar.gz file to a staging area. For
convenience, /tmp is used in these instructions.

2.  Login to the automount host as root or su to root.

3.  Change directory to /tmp and explode the tarball using the commands:
# cd /tmp ↵
# gzip –dc anlpasswd30.tar.gz | tar –xovf - ↵

4.  Change directory to the top level directory and run the install script using the command:
# cd /tmp/anlpasswd ↵
# ./install_anlpasswd.pl ↵

This will install the /tools/bin/anlpasswd30 script with links to
/tools/bin/anlpasswd and /tools/bin/yppasswd, the dictionaries
themselves, and the dictionary indexes.

5.  If you DO have a password aging method in place, skip to step 8. If
you do not have a password aging method in place and are implementing
the password aging script, copy the
/tmp/anlpasswd/password_aging_notify.pl script to the NIS master server.
To implement this script, the following information needs to be edited
in the passwordage.pl script:

# Master NIS server

$master_host = "<NISMASTER>";

###

# Domain (used when building address to send users email)
$domain = "<DAACDOMAIN>";
#
```

```
# Location of the Shadow file
$shadow_file = "<SHADOWFILELOCATION>";

# The protected accounts - these accounts are immune to password aging


@protected_accounts = ('root');
###


# Location of the directory to backup copies of the shadow file in
$shadow_archive = "<SHADOWFILEARCHIVELOCATION>";
###

# Variables used when sendmail emails messages to users and SAs
# This to address is used when sending emails to the SAs
$to_address = "<SAADDRESSLIST>";
```

where:
<NISMASTER> is the fully qualified host name for the NIS master
<DAACDOMAIN> is the NIS domain name of the DAAC
<SHADOWFILELOCATION> is the location of the shadow file (normally /etc/shadow)
<SHADOWFILEARCHIVELOCATION> is the directory of the shadow file archive backups
< SAADDRESSLIST> is the email account(s) to send messages to SAs

6. Setup cron to run the script at a convenient time.

7. Logoff from the automount host.

8. Checkout the SGI installation from an SGI production host by logging in as a normal user.

9. Change your password using the command:

```
      % /tools/bin/yppasswd ↵
```

10. Logout

11. Wait a few minutes to make sure that the updates are completed.

12. Checkout the Solaris installation from a Sun production host by logging in as a normal user.

13. Change your password using the command:

```
      % /tools/bin/yppasswd ↵
```

14. Logout

15. Wait a few minutes to make sure that the updates are completed.

That should be all that is needed to get this program up and running. If there are any problems or inaccuracies in this documentation, or you have any improvements or bug fixes, please send email to "support@mcs.anl.gov"

5.3 Aging Passwords

Password aging is required by NASA NPG 2810.1. A perl script is provided as part of the ANLpasswd 3.0 release that will, after configuration, perform 120-day password aging. If your site already has a method of doing password aging, this section may be ignored. If your site does NOT have a password aging method in place and you are implementing the password aging script, copy the /tmp/anlpasswd/password_aging_notify.pl script to the NIS master server.

To implement this script, the following information needs to be edited in the password_aging_notify.pl script:

```
# Master NIS server
$master_host = "<NISMASTER>";
###

# Domain (used when building address to send users email)
$domain = "<DAACDOMAIN>";
#
# The protected accounts - these accounts are immune to password aging
@protected_accounts = ('root');

# Location of the directory to backup copies of the shadow file in
$shadow_archive = "<SHADOWFILEARCHIVELOCATION>";
###

# Variables used when sendmail emails messages to users and SAs
# This to address is used when sending emails to the SAs
$to_address = "<SAADDRESSLIST>";
```

where:
<NISMASTER> is the fully qualified host name for the NIS master
<DAACDOMAIN> is the NIS domain name of the DAAC
<SHADOWFILELOCATION> is the location of the shadow file (normally /etc/shadow)
<SHADOWFILEARCHIVELOCATION> is the directory of the shadow file archive backups
< SAADDRESSLIST> is the email account(s) to send messages to sys administrators

1 Setup cron to run the script at a convenient time.

2 Logoff from the automount host.

5.4 Secure Access through Secure Shell

The security risks involved in using “R” commands such as rlogin, rsh, rexec and rcp are well known, but their ease of use has made their use tempting in all but the most secure of environments. Ssh is an easy-to-use, drop in replacement for these commands developed by Tatu Ylonen. Ssh is a “user” level application. No changes to the host kernel are required. The UNIX server implements the commercial version of F-Secure. As of the F-Secure 3.2 release, only SSH Version 2 is included in pre-compiled, OS-specific packages

As of the ECS Secure Shell 2.0 release in May, 2000 and later, all of the files needed to function are loaded locally on each UNIX host in /usr/local/bin.

- ssh - replaces rsh, rlogin and rexec for interactive sessions
- scp - replaces rcp for interactive file transfer
- ssh-agent – application that allows a user to enter the passphrase once, then when other applications (e.g. ssh, scp) are used, one is not prompted for the passphrase – it is automatically negotiated.
- ssh-add - add access to a specific ssh host
- ssh-keygen - generates keys for the local host based on a passphrase (long password)
- ssh-signer – verifies that a key is genuine so that public key authentication may proceed
- sftp - secure ftp

The host daemon is in /usr/local/sbin which includes:

- sshd2 - the ssh version 2 daemon

Several files are generated on installation and when running and are installed locally:

- /etc/ssh2/ssh2_config - system-wide configuration for the ssh2 client
- /etc/ssh2/hostkey - contains the long number used for one of the ssh2 keys
- /etc/ssh2/hostkey.pub - contains the ssh2 key known to the public
- /etc/ssh2/random_seed - base number used in generating keys
- /etc/ssh2/sshd2_config - defines the local ssh2 security policy
- /etc/sshd2_22.pid - the process id of the ssh2 daemon currently running

The amount of disk space that the programs and the configurations require is less than 25 MB.

5.4.1 Installation of SSH

The following procedures should be used to install F-Secure SSH 3.2 AND/OR TCP Wrappers 7.6. Both packages are provided as part of the ssh32 release.

5.4.1.1 Sun Installation

The approximate installation time for average systems administrator per host is 15 minutes. The space required is 75MB for install 0-10MB in operations. No reboot is required.

1 Login to host as root or **su** to root.

2 Copy the ssh32.tar.gz file to /tmp or other convenient location (net/admin?).

3 To change to the directory where the ssh32.tar.gz file is located, type **cd /tmp** (or other path if /tmp is not the location to which the file was copied), and then press the **Return/Enter** key.

- The directory is changed to the specified path.

4 To explode the file, type **gzip –dc ssh32.tar.gz | tar –xvf-** and then press the **Return/Enter** key.

- The file is exploded.

5 To change to the ssh32 install directory, type **cd ssh 32**, and then press the **Return/Enter** key.

- The directory is changed to the specified path.

6 To explode the Sun tarfile, type **tar –xvf ssh32.sunpkg.tar** and then press the **Return/Enter** key.

- The file is exploded.

7 To back up the existing files, type **cpssh**, and then press the **Return/Enter** key.

- By default, the files are copied to **/tmp/bssh** and a tar file is created under the name **/tmp/<*hostname*>.bssh24.tar**. *Note*: It is recommended to back up the tar file to another location in the event a problem occurs.

8 To verify that the system has the old versions of ssh, type **pkginfo | grep ssh** and then press the **Return/Enter** key.

- The filenames containing **ssh** are listed. To remove them, go to Step 9.
- ***Note***: If there are no old versions present, skip to Step 11.

9 If the response in Step 8 is positive, to remove the old ssh21 packages, type **pkgrm ssh21** and then press the **Return/Enter** key.

- The removal process function executes; for any questions asked, type **y** and then press the **Return/Enter** key.
- ***Note***: If the removal fails, note the error; if the failure is because a file is missing (a missing file will prevent the removal from completing), copy the file from the backup made in Step 7 and then retry Step 9.

10 To remove the old ssh20 packages, type **pkgrm ssh20** and then press the **Return/Enter** key.

- The removal process function executes; for any questions asked, type **y** and then press the **Return/Enter** key.
- ***Note***: If the removal fails, note the error; if the failure is because a file is missing (a missing file will prevent the removal from completing), copy the file from the backup made in Step 7 and then retry Step 10.

11 To install the new TCP Wrappers package, type **pkgadd –d /tmp/ssh32 tcpw76** and then press the **Return/Enter** key.

- The TCP Wrappers package installation is executed; for any questions asked, type **y** and then press the **Return/Enter** key.

12 To install the new ssh32 package, type **pkgadd –d /tmp/ssh32** and then press the **Return/Enter** key.

- The package installation is executed; for any questions asked, type **y** and then press the **Return/Enter** key.

13 Edit (e.g., using the VI editor) /etc/ssh2/ssh2_config to uncomment the appropriate lines for **SocksServer** (not needed for EDF) and **DefaultDomain**.

14 Edit (e.g., using the VI editor) /etc/ssh2/sshd2_config to uncomment the appropriate line for **AllowSHosts**.

15 If you changed the AllowSHosts line (Step 14), to restart the daemon, type **/etc/init.d/sshd2 restart** and then press the **Return/Enter** key.

- The daemon is restarted.

16 To remove the install directory (as required), type **rm –rf /tmp/ssh32** and then press the **Return/Enter** key.

- The directory is removed.

17 Logoff from **root** and login as a normal user.

18 Do some quick checks to verify the install.

- e.g., Execute the commands **ps –ef | grep sshd2** (should show at least one process spawned recently by PID 1), **ssh2 <*different host*>**, and **scp2 localtestfile remotehost:**.

19 Logoff.

5.4.1.2 SGI Installation

The approximate installation time for average systems administrator per host is 15 minutes. The space required is 75MB for install 0-10MB in operations. No reboot is required.

1 Login to host as root or **su** to root.

2 Copy the ssh32.tar.gz file to /tmp or other convenient location (net/admin?).

3 To change to the directory where the ssh32.tar.gz file is located, type **cd /tmp** (or other path if /tmp is not the location to which the file was copied), and then press the **Return/Enter** key.

- The directory is changed to the specified path.

4 To explode the file, type **gzip –dc ssh32.tar.gz | tar –xvf-** and then press the **Return/Enter** key.

- The file is exploded.

5 To change to the ssh32 install directory, type **cd ssh 32**, and then press the **Return/Enter** key.

- The directory is changed to the specified path.

6 To explode the SGI tarfile, type **tar –xvf ssh32+.sgiinst.tar** and then press the **Return/Enter** key.

- The file is exploded.

7 To back up the existing files, type **cpssh**, and then press the **Return/Enter** key.

- By default, the files are copied to **/tmp/bssh** and a tar file is created under the name **/tmp/<*hostname*>.bssh24.tar**. *Note*: It is recommended to back up the tar file to another location in the event a problem occurs.

8 To verify that the system has the old versions of ssh, type **versions | grep ssh** and then press the **Return/Enter** key.

- The filenames containing **ssh** are listed. To remove them, go to Step 9.
- ***Note***: If there are no old versions present, skip to Step 11.

9 If the response in Step 8 is positive, to remove the old ssh21 packages, type **versions remove ssh21** and then press the **Return/Enter** key.

- The removal process function executes.
- ***Note***: If the removal fails, note the error; if the failure is because a file is missing (a missing file will prevent the removal from completing), copy the file from the backup made in Step 7 and then retry Step 9.

10 To remove the old ssh20 packages, type **versions remove ssh20** and then press the **Return/Enter** key.

- The removal process function executes.
- ***Note***: If the removal fails, note the error; if the failure is because a file is missing (a missing file will prevent the removal from completing), copy the file from the backup made in Step 7 and then retry Step 10.

11 To change to the sgi install directory, type **cd /sgi** and then press the **Return/Enter** key.

- The directory is changed to **/tmp/ssh32/sgi**.

12 To begin installation of the new package, type **inst** and then press the **Return/Enter** key.

- The screen displays a list of choices and the prompt **Inst>**.

13 Type **from** and then press the **Return/Enter** key.

- The screen displays the prompt **Install software from: [<*last used path*>]>**.

14 Type **.** (period) and then press the **Return/Enter** key.

- The screen displays the prompt **Inst>**.

15 Type **step** and then press the **Return/Enter** key.

- The screen displays **N** and the first item in a list of fssh32 and tcpw76 modules, with the cursor at beginning of the line (in front of the **N**).

- *Note*: The **N** indicates "New" and what is typically displayed – i.e., the module is not installed. If there were an earlier version of the module installed, the display would show **U** (i.e., installing the module would be an "Upgrade"). If the module were already installed, the display would show **S** (i.e., installing the module would install the "Same" version). If there were a later version of the module installed, the display would show **D** (i.e., installing the module would be a "Downgrade").

16 To indicate that the module is to be installed, type **i** and then press the **Return/Enter** key.

- The letter **i** is displayed at the beginning of the line for the module and the next module in the list is displayed, with the cursor at the beginning of its line (in front of the **N**).
- *Note*: If this is the last module in the list, the screen displays a disk space summary and the prompt **Inst>**.

17 Repeat Step 16 as needed until the letter **i** is displayed in front of each module in the list.

18 Type **go** and then press the **Return/Enter** key.

- The installation is executed; for any questions asked, type **y** and then press the **Return/Enter** key. There should be *no* conflicts.
- The screen displays the prompt **inst>**.

19 Type **quit** and then press the **Return/Enter** key.

- The install is complete.

20 Edit (e.g., using the VI editor) /etc/ssh2/ssh2_config to uncomment the appropriate lines for **SocksServer** (not needed for EDF) and **DefaultDomain**.

21 Edit (e.g., using the VI editor) /etc/ssh2/sshd2_config to uncomment the appropriate line for **AllowSHosts**.

22 If you changed the AllowSHosts line (Step 21), to restart the daemon, type **/etc/init.d/sshd2 restart** and then press the **Return/Enter** key.

- The daemon is restarted.

23 To remove the install directory (as required), type **rm –rf /tmp/ssh32** and then press the **Return/Enter** key.

- The directory is removed.

24 Logoff from **root** and login as a normal user.

23 Do some quick checks to verify the install.

- e.g., Execute the commands **ps –ef | grep sshd2** (should show at least one process spawned recently by PID 1), **ssh2 <*different host*>**, and **scp2 localtestfile remotehost:**.

25 Logoff.

5.4.2 The SSH Encryption Mechanism[1]

Each host has a host-specific DSA key (normally 1024 bits) used to identify the host. Additionally, when the daemon starts, it generates a server DSA session key (normally 768 bits). This key is normally regenerated every hour if it has been used, and is never stored on disk.

Whenever a client connects the daemon, the daemon sends its host and server public keys to the client. The client compares the host key against its own database to verify that it has not changed. The client then generates a 256 bit random number. It encrypts this random number using both the host key and the server key, and sends the encrypted number to the server. Both sides then start to use this random number as a session key that is used to encrypt all further communications in the session. The rest of the session is encrypted using a conventional cipher. Currently, IDEA, DES, 3DES, and ARCFOUR are supported. Within ECS, 3DES is used by default but is being replaced by aes128 as of the F-Secure 3.2 release. The client selects the encryption algorithm to use from those offered by the server.

Next, the server and the client enter an authentication dialog. The client tries to authenticate itself using .rhosts authentication, .rhosts authentication combined with DSA host authentication, RSA challenge-response authentication, or password based authentication. (NOTE: In the ECS configuration, .rhosts is NOT available).

Rhosts authentication is disabled within the DAACs because it is fundamentally insecure.

If the client successfully authenticates itself, a dialog for preparing the session is entered. At this time the client may request things like allocating a pseudo-tty, forwarding X11 connections, forwarding TCP/IP connections, or forwarding the authentication agent connection over the secure channel.

5.4.3 How a User Uses Secure Shell

The Simplest Way

1 To login, use the command:

```
% slogin defiant ↵
```

```
Enter the passphrase for the key (lotsofstuffhere): br0wn cow 3ats grass ↵
Last login: Sun Feb 22 06:50:59 1998 from echuser.east.hitc.com
No mail.
%
```

NOTE: The first time you login to a host the following message will pop up asking if you want to continue. In response, type **yes** and [**enter**]:

[1] From the *sshd* man page

```
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes ↵
Host 't1acg01' added to the list of known hosts.
```

2 To transfer a file, use the command:

```
% scp hostone:/etc/info info ↵
Enter the passphrase for the key (lotsofstuffhere):  br0wn cow 3ats grass ↵
```

- This will copy the file /etc/info from hostone to your local host. Note that your passphrase is needed to initiate the transfer.

IMPORTANT NOTE: The default directory on the *target* host is always the users HOME directory.

3 Also, one may send/receive files recursively using "-r" such as:

```
% scp -r ~/files/* hostone:~/files ↵
```

will send what is in the home directory files subdirectory to the target host hostone in the home files subdirectory.

4 To execute a command remotely, use the command:

```
% ssh whoisonfirst ps –ef ↵
Enter the passphrase for the key (lotsofstuffhere):  br0wn cow 3ats grass ↵
```

5.4.4 A Layer of Convenience

If you are already a user of "r" commands, you probably know about the .rhost file. Ssh will allow a user to setup the .rhost equivalent called .shost in one's home directory. .Rhost and .shost contain the names of the hosts to which one normally connects. The nice thing about using it is one need not enter one's passphrase. Unlike "r" commands, however, ssh commands use long strings of numbers to authenticate the client, which makes it quite difficult for an intruder to impersonate a legitimate user. One word of caution, however, if you leave your terminal while logged on, a passerby could logon to any host in your .rhost/.shosts file and potentially cause malicious damage to you and your colleagues work. Be aware!

NOTE: ssh checks the mode of .shost, so change permission on .shost by typing:

```
% chmod 600 /home/JohnDoe/.shost ↵
```

where you must substitute your own home directory for /home/JohnDoe.

5.4.5 Multiple Connections

If you open multiple connections, it is more convenient to keep your keys in system memory. To do this requires executing two commands:

```
% ssa ↵
Enter the passphrase for the key (lotsofstuffhere):
Enter passphrase: br0wn cow 3ats grass ↵
Identity added: /home/JohnDoe/.ssh/identity (bpeters@nevermor)
%
```

Now, one may make connections (slogin, scp, ssh) to hosts that are running ssh without being prompted for a passphrase.

5.4.6 Secure FTP

As of this release, a secure version of ftp is included. Use the command:

```
% sftp user@remotehost ↵
Enter the passphrase for the key (lotsofstuffhere): MY PASSPHRASE ↵
local directory - /home/user
remote directory - /home/user
sftp> get thisisafilename ↵
sftp> put thisotherfilename ↵
sftp> quit ↵
```

5.4.7 Other Notes

IMPORTANT: Ssh will automatically "tunnel" X sessions without user involvement even through multiple hops. However, it is important that you do NOT change the DISPLAY parameter or X will not use the ssh tunnel!

5.4.8 Configuration of Secure Shell

5.4.8.1 Local Setup

Most users will start from the same host whether from an X terminal, a UNIX workstation, or a PC. Running the ssa (sshsetup) script generates long strings called keys that make ssh work. One set of keys is needed for each home directory.

The only thing you need to know before executing the script is to pick a good passphrase of at least 10 characters. You can and should use spaces and multiple words with numbers, misspellings and special characters. Note that passwords are NOT echoed back to the screen.

PLEASE DO NOT USE THE PASSWORDS/PASSPHRASES USED HERE OR IN ANY OTHER DOCUMENTATION!

Using the script ssa should look like:

```
% ssa ↵
Use a passphrase of at least 10 characters; which should include numbers
or special characters and MAY include spaces
New passphrase: This is a silly test ↵
```

```
Retype new passphrase: This is a silly test ↵
Generating ssh1 keys. Please wait while the program completes...
Generating ssh2 keys. This can take up to 240 seconds...
Done with sshsetup!
%
```

You are on the way!

NOTE: If you have accounts in the PVC, VATC and/or the EDF, at a DAAC production LAN or DAAC M&O LAN, do ssa in EACH environment.

5.4.8.2 Remote Setup

If you need to access a host with a different home directory, you will need to run the ssr (ssh remote) script. NOTE: It is helpful to have run Secure Shell Setup (sss) in each environment first before doing the ssh remote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. A new capability is to use different user names on the source and target hosts. This should look something like:

```
% ssr ↵
Remote user name (default: yourusername): ↵
Do you want to setup for:
1  VATC
2  PVC
3  MiniDAAC
4  GSFC DAAC
5  SMC
6  GSFC M and O
7  EDC DAAC
8  EDC M and O
9  LaRC DAAC
10   LaRC M and O
11  NSIDC DAAC
12  NSIDC M and O
x  Exit from script
Select:
2
Working...
Accepting host p0spg07.pvc.ecs.nasa.gov key without checking.
yourusername@p0spg07.pvc.ecs.nasa.gov's password:
Authentication complete. Continuing with sshremote...
Downloaded remote keys.
Uploaded local keys.
Keys concatenated.
```

```
Enter next site (press the enter-key and then x enter-key to exit)
Remote user name (default: yourusername):  ↵

Do you want to setup for:
1   VATC
2   PVC
3   MiniDAAC
4   GSFC DAAC
5   SMC
6   GSFC M and O
7   EDC DAAC
8   EDC M and O
9   LaRC DAAC
10   LaRC M and O
11  NSIDC DAAC
12  NSIDC M and O
x   Exit from script
Select:
x <enter>
bye!
%
```

5.4.8.3 Changing your Passphrase

To change your passphrase, use the following command:

```
% ssp ↵

Enter old passphrase: little 1amp jumb3d <enter>
Enter a  new passphrase of at least 10 characters which should include
numbers or special characters and MAY include spaces

New passphrase: br0wn cows 3at grass  ↵
Retype new passphrase: br0wn cows 3at grass ↵

ssh2 key changed successfully.
Done with sshpass2!
```

5.4.9 Administration of Secure Shell

There is no administration of secure shell required except for general monitoring to make sure that the daemon process (/usr/local/sbin/sshd2) is running. Note, however, that the standard installation will establish a /var/log/ssh log file. It is recommended to review the /var/log/ssh and the system log file at least once a week.

5.5 Controlling Requests for Network Services (TCP Wrappers)

With TCP Wrappers, you can monitor and filter incoming requests for network services, such as FTP.

TCP Wrapper provides a small wrapper program for inet daemons that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client host and the name of the requested service; the wrappers do not exchange information with the client or server applications, and impose no overhead on the actual conversation between the client and server applications. The usual approach is to run one single daemon process that waits for all kinds of incoming network connections. Whenever a connection is established, this daemon runs the appropriate server program and goes back to sleep, waiting for other connections.

Operations personnel will monitor requests for these network services:

Client	**Server**	**Application**
ftp	Ftpd	file transfer
finger	Fingerd	show users

The **/var/log/wrappers log** file should be reviewed at least once a week. The log file provides information concerning who tried to access the network service. TCP Wrapper blocks any request made by unauthorized users. TCP Wrapper can be configured to send a message to any administrator whose request is rejected.

5.5.1 Installation, Configuration, and Testing for Wrappers

The installation of TCP Wrappers is part of the ECS Secure Shell 2.0 and later packages. As of F-Secure SSH 3.2, it is a separate package and should be installed as part of the ssh installation. See Section 5.4.1 above. The location of most of the wrappers files have been changed to /etc/wrappers. Libwrap.a is in /usr/local/lib and tcpd.h is in /usr/local/include. The installation is automatic if wrappers has been previously installed. After installation, however, the following checks should be made.

1 There are two files that provide access control for the system: /etc/hosts.allow and /etc/hosts.deny

- The general format is:

  daemonlist : clientlist : script : ALLOW/DENY

- What follows is an example of a /etc/hosts.allow file:

```
================
sshd2,sshdfwd-X11,telnetd,ftpd: 127.0.0. : BANNERS /etc/wrappers/banners :
ALLOW
sshd2,sshdfwd-X11,ftpd: 155.157. : BANNERS /etc/wrappers/banners : ALLOW
ALL: ALL:       BANNERS /etc/wrappers/banners : DENY
```

2 Verify that the following lines are included in a Solaris /etc/inetd.conf :

```
ftp    stream  tcp    nowait  root    /etc/wrappers/tcpd     in.ftpd
telnet  stream  tcp    nowait  root    / etc/wrappers/tcpd    in.telnetd
```

- Verify that the default daemons are commented out:

```
#ftp    stream  tcp    nowait  root    /usr/sbin/in.ftpd      in.ftpd
#telnet stream  tcp    nowait  root    /usr/sbin/in.telnetd    in.telnetd
```

3 The following lines should be included in an IRIX /etc/inetd.conf:

```
ftp    stream  tcp    nowait  root    /etc/wrappers/tcpd     ftpd –lll
telnet  stream  tcp    nowait  root    / etc/wrappers/tcpd    telnetd
```

- The default daemons should be commented out:

```
#ftp    stream  tcp    nowait  root    /usr/etc/ftpd      ftpd –lll
#telnet stream  tcp    nowait  root    /usr/etc/telnetd    telnetd
```

4 Verify that wrappers is functioning by telnetting to the installed system from a different local host. (telnet is turned off from the outside). You should get a banner and a log entry.

5 You are done.

5.6 Monitoring File and Directory Integrity (Tripwire)

Tripwire is a tool that aids in the detection of unauthorized modification of files resident on Unix systems. One important application of Tripwire is its use as the first and most fundamental layer of intrusion detection for an organization. Tripwire is automatically invoked at system startup. This utility will check the file and directory integrity by comparing a designated set of files and directories against information stored in a previously generated database. Tripwire flags and logs any differences, including added or deleted entries. When run against system files regularly, Tripwire spots any changes in critical system files, records these changes into its database, and notifies system administrators of corrupted or tampered files so that they can take damage control measures quickly and effectively. With Tripwire, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes. Tripwire works in conjunction with these other solutions to provide a "Defense in Depth"(trademark) security solution.

NOTE: Since system files should not change and users' files change constantly, Tripwire should be used to **monitor only system files**. The list of system files you want to monitor is stored in **./configs/tw.conf**.

The system administrator should install Tripwire on a clean system. This baseline database will then be used to compare possible changes to files and directories to make sure the system has not been compromised. If the system has been compromised, information provided by Tripwire can be used to carry out a forensics investigation of the compromise. Forensics is the compiling of the chain of evidence necessary to prosecute offenders after an attack has occurred.

The system administrator should check any changes made to the system on a weekly basis or after an alert from a security organization like NASIRC or CERT has put out an alert on security vulnerabilities for any of the baseline operating systems or COTS software.

All reported changes need to be investigated right away. The investigator should be aware that most of the file changes are due to system updates. But each change should be traceable to a specific, baselined change. If no unexplained changes are detected, then the Tripwire database needs to be updated to reflect file updates. Tripwire should be configured to mail the system administrator any output that it generates.

5.6.1 Installation of Tripwire

1 Login or **su** to root.

2 Change directory to the admin automount:

```
# cd /tools/admin
```

3 Make a tripwire directory using the command:

```
# mkdir tripwire
```

4 Make sun5, and irix 65 directories:

```
# mkdir sun5

# mkdir irix65
```

5 Download the distributions from the SMC to their respective directory and uncompress.

6 Copy inetd file using the command:

```
# cp /etc/inet/inetd.conf /etc/inet/inetd.conf.orig ↵
```

7 To setup:

```
# /etc/tripwire-1.2/src/tripwire -init ↵
```

- This will create a database file in:
  /etc/tripwire-1.2/src/databases/tw.db_HOSTNAME

8 To test, from a normal user account, execute the command:

```
% touch /etc/intruder
```

9 From root, then get the report using the command:

```
# /etc/tripwire-1.2/src/tripwire -v > /tmp/tw.report
```

- This should report /etc/intruder was created.

10 Delete the test file and the sample reports using the commands:

```
# rm /etc/intruder

# rm /tmp/tw.report
```

5.6.2 Updating the Tripwire Database

You can update your Tripwire database in two ways. The first method is interactive, where Tripwire prompts the user whether each changed entry should be updated to reflect the current state of the file, while the second method is a command-line driven mode where specific files/entries are specified at run-time.

5.6.2.1 Updating Tripwire Database in Interactive Mode

Running Tripwire in Interactive mode is similar to the Integrity Checking mode. However, when a file or directory is encountered that has been added, deleted, or changed from what was recorded in the database, Tripwire asks the user whether the database entry should be updated.

For example, if Tripwire is run in Interactive mode and a file's timestamp changed, Tripwire will print out what it expected the file to look like, what it actually found, and then prompt the user to specify whether the file should be updated. For example:

```
/etc/hosts.equiv
    st_mtime: Wed May  5 15:30:37 1993     Wed May  5 15:24:09 1993
    st_ctime: Wed May  5 15:30:37 1993     Wed May  5 15:24:09 1993
---> File:  /etc/hosts equiv
---> Update entry?  [YN(y)n?] y ↵
```

You could answer yes or no, where a capital 'Y' or 'N' tells Tripwire to use your answer for the rest of the files. (The 'h' and '?' choices give you help and descriptions of the various inode fields.)

While this mode may be the most convenient way of keeping your database up-to-date, it requires that the user be "at the keyboard." A more conventional command-line driven interface exists, and is described next.

5.6.2.2 Updating Tripwire Database in Database Update Mode

Tripwire supports incremental updates of its database on a per-file/directory or tw.config entry basis. Tripwire stores information in the database so it can associate any file in the database with the tw.config entry that generated it when the database was created.

Therefore, if a single file has changed, you can:

```
# tripwire -update /etc/newly.installed.file ↵
```

Or, if an entire set of files that made up an entry in the tw.config file changed, you can:

```
# tripwire -update /usr/local/bin/Local_Package_Dir ↵
```

In either case, Tripwire regenerates the database entries for every specified file. A backup of the old database is created in the **./databases** directory.

Tripwire can handle arbitrary numbers of arguments in Database Update mode.

The script **twdb_check.pl** script is an interim mechanism to ensure database consistency. Namely, when new entries are added to the tw.config file, database entries may no longer be associated with the proper entry number. The twdb_check.pl script analyzes the database, and remaps each database entry with its proper tw.config entry.

5.6.3 Configuring the tw.config File

Edit your **tw.config** file in the **./configs** directory, or whatever filename you defined for the Tripwire configuration file, and add all the directories that contain files that you want monitored. The format of the configuration file is described in its header and in the "man" page. Pay especially close attention to the select-flags and omit-lists, which can significantly reduce the amount of uninteresting output generated by Tripwire. For example, you will probably want to omit files like mount tables that are constantly changed by the operating system.

Run Tripwire with **tripwire -initialize**. This will create a file called **tw.db_[hostname]** in the directory you specified to hold your databases (where [hostname] will be replaced with your machine hostname).

Tripwire will detect changes made to files from this point on. You ***must*** be certain that the system on which you generate the initial database is clean; however, Tripwire cannot detect unauthorized modifications that have already been made. One way to do this would be to take the machine to single-user mode, reinstall all system binaries, and run Tripwire in initialization mode before returning to multi-user operation.

This database must be moved someplace where it cannot be modified. Because data from Tripwire is only as trustworthy as its database, choose this with care. It is recommended to place all the system databases on a read-only disk (you need to be able to change the disk to writeable during initialization and updates, however), or exporting it via read-only NFS from a "secure-server." (This pathname is hardcoded into Tripwire. Any time you change the pathname to the database repository, you must recompile Tripwire. This prevents a malicious intruder from spoofing Tripwire into giving a false "okay" message.)

We also recommend that you make a hardcopy printout of the database contents right away. In the event that you become suspicious of the integrity of the database, you will be able to manually compare information against this hardcopy.

Once you have your database set up, you can run Tripwire in Integrity Checking mode by typing **tripwire** on the command line from the directory in which Tripwire has been installed.

5.7 Reporting Security Breaches

Reporting of Security breaches shall be in accordance with NASA Procedures and Guidelines (NPG) 2810.1 (dated August 26,1999 to August 26, 2004). The specific location in the 2810 is Chapter 4, Section 4.4, IT Security Incidents Reporting and Handling.

5.8 Initiating Recovery from Security Breaches

Recovery from Security breaches shall be in accordance with NASA Procedures and Guidelines (NPG) 2810.1 (dated August 26,1999 to August 26, 2004). The specific location in the 2810 is Chapter 4, Section 4.4, IT Security Incidents Reporting and Handling.

6. Network Administration

This section covers the procedures necessary for the management operations that monitor and control the system network capabilities.

Detailed procedures for tasks performed by the Network Administrator are provided in the sections that follow. The procedures assume that the administrator is authorized and has proper access privileges to perform the tasks (i.e., root).

6.1 Network Documentation

ECS Network Administration requires access to restricted documents not available via the cmdm.east.hitc.com (PETE Server) URL. These documents include:

• Network Overview Diagram	921-TDx-001
(x = DAAC designation: G/Goddard; L/Langley; N/NSIDC; E/EDC)	
• Hardware Network Diagram	921-TDx-002
• Host IP Assignments	921-TDx-003
• Network IP Assignments	921-TDx-004
• Dual-Homed Host Static Routes	921-TDx-005
• Ingest Host Static Routes	921-TDx-006

These documents describe and depict the network layout and inter/intra-connections necessary to understand the ECS. Contact Landover Configuration Management for copies for individual sites.

6.2 Network Monitoring

WhatsUp Gold (Version 8.0) is a graphical network monitoring application selected to monitor critical devices and services on the ECS Production Local Area Network (LAN) and/or additional ECS networks. It initiates alerts when it detects problems, and can send remote notifications by beeper, pager, and e-mail. It logs events to facilitate troubleshooting and reporting. It is implemented on Windows 2000 on a Personal Computer (PC) connected to the Production LAN. Chapter 7 of this document provides basic procedures for WhatsUp Gold. Detailed configuration and installation instructions are available in Document 914-TDA-246 *WhatsUp Gold 8.0 for the ECS Project, Release Notes*, and in the following vendor documents:

- *WhatsUp Gold version 8 User's Guide* accessible on the internet and downloadable at http://support.ipswitch.com/kb/WG-20030121-DM01.htm

Monitoring is also conducted via command-line interaction and site-developed scripts. An overview of network information is provided here as a basis for evaluating network status.

6.3 DAAC LAN Topology Overview

The Distributed Active Archive Center (DAAC) Local Area Network (LAN) consists of a Portus Firewall, a Production/Ingest Ethernet Network, and a Gigabit Ethernet (GigE) Network. There are variations in the topology at the different sites. Note: The NSIDC DAAC does not have a Production network.

The Firewall and separate Processing network allow processing flows to be unaffected by user pull demands, and the introduction of the high-speed GigE Network provides adequate bandwidth to the Processing and Data Server subsystems to transfer high volumes of data. Each of the networks is discussed in detail below.

6.3.1 The Production Network

The Production Network consists of a Catalyst 6006 Ethernet switch supporting the DAAC subsystems. EOS Mission Support network (EMSn) [formerly EOSDIS Backbone Network (Ebnet)] connections to external production systems such as EDOS and other ECS DAACs are made by means of the DAAC's ECS router. A connection in the ECS router provides access to the EMSn router to handle DAAC-DAAC flows.

6.3.2 The Firewall

The Firewall connects users (e.g., via NISN, local campuses, Abilene, general Internet) to the DAAC Ethernet to provide user access. It separates user and production flows. This allows DAAC processing data flows to be unaffected by user demand so that even unanticipated user pull will not hinder the production network. The Firewall provides access to Data Manager hosts and to a subset of DataServer hosts that interact with users. Users will not have access to any other hosts such as Ingest or Processing devices. CSS and MSS servers are also connected to the Ethernet. These servers are required for communications with outside networks for such things as name lookups and receipt of Internet mail as well as communication with and monitoring of the DAAC's interfaces to the user community (such as NISN and the local campus).

The Firewall connects to the Campus Isolation LAN through an Ethernet 6006 switch and ECS router, which provides the necessary routing and filtering controls. NISN, the local Campus, and other Internet providers will also be connected to the Campus Isolation LAN.

6.3.3 Ethernet Topology

All hosts within a DAAC are connected to the Catalyst 6006 Ethernet switch. This switch is used to connect hosts at 10/100/100 Mb/s. The Catalyst 6006 Ethernet switch is also connected to the ECS router via a 1000Mb/s circuit.

6.4 Network Hardware Components

6.4.1 LAN Components

The DAAC LANs consist of the following hardware components:

Portus Firewall. The Portus Firewall hardware consists of an IBM RS6000 server installed with the basic AIX 4.3.3 operating system. It contains 2 9GB internal disk drives that are mirrored, as well as a pair of redundant power supplies. E-Border Server COTS product has been installed to correct/enhance the window sizing issues with the RS6000 IBM server.

Access Server. The Access Server is a Cisco 2509. It consist of eight modem ports and an Ethernet port.

Maintenance and configuration of the access server is considered a non-trivial function. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by ECS.

ECS Router. The ECS Router is a Cisco 7507 or 7513. It is a high-speed interface (1000 Mbps). It consists of several FDDI and Ethernet interfaces. It interfaces to EMSnet, the local campus network, NI, M&O network, User network, and Production network. It provides IP address and port level filtering in support of the ECS security policy.

Maintenance and configuration of the ECS router is considered a non-trivial function. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by ECS.

Ethernet Switch. The Ethernet switch is a Cisco catalyst 6006. It provides a large number of 10/100/1000 MB/sec interfaces. It interfaces to all Production hosts and to the ECS router. Maintenance and configuration of the Ethernet Switch is considered a non-trivial function. Such tasks are addressed in special technical training provided by the vendor and supplemental training provided by ECS.

6.5 ECS Domain Name Services (DNS) Structure

The parent DNS domain for ECS is **ecs.nasa.gov**. These DNS servers reside at the SMC, NSIDC, and EDC. In this domain are the SMC hosts, User hosts for all DAACs, and pointers to the DAACs' DNS servers. The external DNS resides on the Portus Firewall.

The ecs.nasa.gov DNS servers are:

- m0mss02.ecs.NASA.GOV (internet address = 198.118.212.37).
- m0mss04.ecs.NASA.GOV (internet address = 198.118.212.41).
- n0css02u.ecs.NASA.GOV (internet address = 198.118.206.84).
- e0css02u.ecs.NASA.GOV (internet address = 198.118.203.104).

The DAACs' Production networks are a child domain of ecs.nasa.gov. They are:

- LaRC Production networks:
  - l0ins02.larcb.ecs.nasa.gov (internet address = 198.118.219.74).
  - l0css02.larcb.ecs.nasa.gov (internet address = 198.118.219.67).
- EDC (LPDAAC) Production networks:
  - e0ins02.edcb.ecs.nasa.gov (internet address = 198.118.202.159).

  - e0css02.edcb.ecs.nasa.gov (internet address = 198.118.202.132).
- NSIDC Production network:
  - n0ins02.nsidcb.ecs.nasa.gov (internet address = 198.118.205.145).
  - n0css02.nsidcb.ecs.nasa.gov (internet address = 198.118.205.123).
- GSFC Production networks:
  - g0ins02.gsfcb.ecs.nasa.gov (internet address = 198.118.210.69).
  - g0css02.gsfcb.ecs.nasa.gov (internet address = 198.118.210.63).

The DAACs' M&O networks are also a child domain of ecs.nasa.gov. They are:

- LaRC M&O network.
  - larcmo.ecs.nasa.gov
- EDC M&O network.
  - edcmo.ecs.nasa.gov
- NSIDC M&O network.
  - nsidcmo.ecs.nasa.gov
- GSFC M&O network.
  - gsfcmo.ecs.nasa.gov

6.6 Host Names

A letter is appended to the production host name to distinguish which interface (and IP address) a user is accessing.

As an example, a GSFC DAAC host named g0acg01.gsfcb.ecs.nasa.gov is a host attached to the Production network.

6.7 Network Security

6.7.1 ECS Network Connectivity

The ECS network was designed to minimize unauthorized user access, including the use of a Firewall at each site. Ingest network access at a DAAC is limited to its Level 0 data provider(s), the SMC, and hosts attached to the DAAC's Production and M&O networks. No local campus, Internet or other DAAC access is provided. Access to a DAAC's Production network is limited to the SMC, the DAAC's M&O network, and other DAACs. No local campus, Internet, or Level 0 data provider(s) access is provided.

6.7.2 Troubleshooting - Verifying connectivity

One of the key reasons for failure of data access and transfer is an error or problem in system connectivity. This can be caused by a myriad of glitches such as incorrect/outdated lookup tables, incorrectly assigned IP addresses, missing default route and more. Besides checking individual host/server operation with various tools such as ECS Assistant, you can use several command line entries to verify point-to-point communication between components.

There are three initial steps to help verify system connectivity. They include ensuring connectivity is authorized, determining if the Domain Name Service (DNS) is resolving host name and IP addresses correctly, and actively testing the connectivity by using the ping function. Authorized connectivity can be determined by checking the ECS Network Connectivity matrix.

6.7.2.1 Checking local host access to another local host over the network

1 On workstation ***x0xxx##,*** at the UNIX prompt in a terminal window, check the Domain Name Service entries (DNS) for the source host by typing **nslookup < local_host>**.

- The screen display will be similar to the following:

```
g0spg01{mblument}[204]->nslookup g0spg01
Server:  g0css02.gsfcb.ecs.nasa.gov
Address:  198.118.210.63
 Name:    g0spg01.gsfcb.ecs.nasa.gov
Address:  198.118.210.16
```

2 Check the DNS entries for the remote host by typing **nslookup <other host>.**

- The screen display will be similar to the following:

```
g0spg01{mblument}[201]->nslookup g0css02
Server:  g0css02.gsfcb.ecs.nasa.gov
•   Address:  198.118.210.63
 Name:    g0css02.gsfcb.ecs.nasa.gov
Address:  198.118.210.63
```

3 Determine the host's network interface using **ifconfig <interface>** where **<interface>** parameter can be found by executing **netstat -i**

- The **netstat -i** command will provide the following information:

```
g0spg01{mblument}[201]->netstat -i
Name Mtu   Network     Address          Ipkts Ierrs   Opkts Oerrs  Coll
ipg0 4352  198.118.210 g0spg01.gsfcb.   9182666    1  8103032    0    0
hip0 65280 192.168.1   g0spg01h.gsfcb.  5554524    0  6776651    0    0
xpi0 4352  198.118.212.64 g0spg01u.ecs.  37850320    0 14109683    3    0
xpi1 0     none        none             0    0       0    0    0
et0* 1500  none        none              0    0       0    0    0
lo0  8304  loopback    localhost        314800    0  314800    0    0
```

- Using **ipg0** from the **ifconfig <interface>** data as the interface parameter, **ifconfig ipg0**, will result in the following display:

```
g0spg01{mblument}[203]->ifconfig ipg0
ipg0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>
inet 198.118.210.16 netmask 0xffffff00 broadcast 198.118.210.255
```

4 Ping the two hosts to verify their inter-connectivity.

- Ping the local host (g0spg01).

```
g0spg01{mblument}[232]->ping g0spg01
PING g0spg01.gsfcb.ecs.nasa.gov (198.118.210.16): 56 data bytes
64 bytes from 198.118.210.16: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 198.118.210.16: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 198.118.210.16: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 198.118.210.16: icmp_seq=3 ttl=255 time=0 ms
64 bytes from 198.118.210.16: icmp_seq=4 ttl=255 time=0 ms
 ----g0spg01.gsfcb.ecs.nasa.gov PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
g0spg01{mblument}[233]->
```

- Ping the remote host (g0css02).

```
g0spg01{mblument}[202]->ping g0css02
PING g0css02.gsfcb.ecs.nasa.gov (198.118.210.63): 56 data bytes
64 bytes from 198.118.210.63: icmp_seq=0 ttl=255 time=2 ms
64 bytes from 198.118.210.63: icmp_seq=1 ttl=255 time=1 ms
64 bytes from 198.118.210.63: icmp_seq=2 ttl=255 time=1 ms
64 bytes from 198.118.210.63: icmp_seq=3 ttl=255 time=1 ms
64 bytes from 198.118.210.63: icmp_seq=4 ttl=255 time=1 ms
 ----g0css02.gsfcb.ecs.nasa.gov PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1/1/2 ms
```

5 Check the health of the interface by executing **netstat -i,** looking for Ierrs and/or Oerrs that if present (1 or 2 errors are ok, 100 are not ok) indicate an interface problem; check the syslog for any startup or logged problems from the OS.

```
g0spg01{mblument}[218]->netstat -i
Name Mtu   Network     Address           Ipkts        Ierrs        Opkts        Oerrs  Coll
ipg0 4352  198.118.210 g0spg01.gsfcb.    9197317      1            8113487      0      0
hip0 65280 192.168.1   g0spg01h.gsfcb.   5554541      0            6776668      0      0
xpi0 4352  198.118.212.64 g0spg01u.ecs.  37851779     0            14109837     3      0
xpi1 0     none        none              0            0            0            0      0
et0* 1500  none        none              0            0            0            0      0
lo0  8304  loopback    localhost         325510       0            325510       0      0
```

6 Check the routing table for accuracy and completeness by executing **netstat -rn.**

- The resultant display will be similar to the following:

```
g0spg01{mblument}[226]->netstat -rn
Routing tables
 Internet:
Destination     Gateway          Netmask   Flags   Refs    Use  Interface
default       198.118.212.65               UGS       1 14060556  xpi0
127.0.0.1       127.0.0.1                UH         7   270097  lo0
```

```
192.168.1        192.168.1.1        0xffffff00 U         0        0  hip0
192.168.1.1      192.168.1.1                   UGHS      0       22  hip0
192.168.1.2      192.168.1.2                   UGHS      1  3993577  hip0
192.168.1.3      192.168.1.3                   UGHS      0       17  hip0
192.168.1.4      192.168.1.4                   UGHS      0  2397593  hip0
192.168.1.5      192.168.1.5                   UGHS      2      178  hip0
192.168.1.6      192.168.1.6                   UGHS      0       24  hip0
192.168.1.7      192.168.1.7                   UGHS      0     1403  hip0
192.168.1.8      192.168.1.8                   UGHS      0        6  hip0
192.168.1.9      192.168.1.9                   UGHS      0        0  hip0
192.168.1.10     192.168.1.10                  UGHS      0        0  hip0
198.118.198      198.118.210.1      0xffffff00 UGS       0       16  ipg0
198.118.198.12   198.118.210.2                 UGHD      0    31646  ipg0
198.118.198.14   198.118.210.2                 UGHD      0     1032  ipg0
198.118.198.17   198.118.210.2                 UGHD      0        0  ipg0
198.118.198.25   198.118.210.2                 UGHD      0      194  ipg0
198.118.198.26   198.118.210.2                 UGHD      0    36153  ipg0
198.118.198.27   198.118.210.2                 UGHD      0    23425  ipg0
198.118.198.28   198.118.210.2                 UGHD      4    11686  ipg0
198.118.198.29   198.118.210.2                 UGHD      0     1682  ipg0
198.118.198.30   198.118.210.2                 UGHD      3    14760  ipg0
198.118.198.32   198.118.210.2                 UGHD      2   917384  ipg0
198.118.198.42   198.118.210.2                 UGHD      0    87381  ipg0
198.118.198.76   198.118.210.2                 UGHD      3   568062  ipg0
198.118.198.100  198.118.210.2                 UGHD      0     1223  ipg0
198.118.198.107  198.118.210.2                 UGHD      0      299  ipg0
198.118.198.113  198.118.210.2                 UGHD      0      893  ipg0
198.118.198.116  198.118.210.2                 UGHD      0     9438  ipg0
198.118.202      198.118.210.1      0xffffff00 UGS       0        0  ipg0
198.118.205      198.118.210.1      0xffffff00 UGS       0        0  ipg0
198.118.208      198.118.210.1      0xffffff00 UGS       0        0  ipg0
198.118.210      198.118.210.16     0xffffff00 U       177  5624292  ipg0
198.118.210.16   127.0.0.1                     UGHS     15    55462  lo0
198.118.211.32   198.118.210.1      0xffffffe0 UGS       0     6842  ipg0
198.118.212.32   198.118.210.1      0xffffffe0 UGS       0     1004  ipg0
198.118.212.40   198.118.210.2                 UGHD      0     6205  ipg0
198.118.212.64   198.118.212.69     0xffffffe0 U         0     4485  xpi0
198.118.212.160  198.118.210.1      0xffffffe0 UGS       0        0  ipg0
198.118.219      198.118.210.1      0xffffff00 UGS       0        0  ipg0
198.118.220      198.118.210.1      0xffffff00 UGS       0        0  ipg0
```

```
198.118.232      198.118.210.1      0xffffff00 UGS        0      143  ipg0
210.138.100      198.118.210.1      0xffffff00 UGS        0        0  ipg0
224          198.118.210.16     0xf0000000 US         0        2  ipg0
g0spg01{mblument}[227]->
```

- Ping the default IP address to ensure connectivity to the default route (default: 198.118.212.65)

```
g0spg01{mblument}[228]->ping 198.118.212.65
PING 198.118.212.65 (198.118.212.65): 56 data bytes
64 bytes from 198.118.212.65: icmp_seq=0 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=1 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=2 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=3 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=4 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=5 ttl=255 time=1 ms
64 bytes from 198.118.212.65: icmp_seq=6 ttl=255 time=1 ms
 ----198.118.212.65 PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 1/1/1 ms
```

7 Check the other host using the same steps.

8 Check other hosts using the same infrastructure components as the two hosts with the problem.

9 If the host you are trying to communicate with is attached to the Ethernet Hub, make sure that the "Don't Fragment" bit in the IP header is NOT set on the host which is FDDI attached. The Ethernet Hub does not support Maximum Transfer Unit (MTU) discovery so it will not inform the host that the packet is too big. It silently discards the packet. By default, the Sun hosts are improperly configured. Check the file /etc/init.d/inetinit to ensure that the command to reset the "Don't Fragment" bit is included: **ndd -set /dev/ip ip_path_mtu_discovery 0**

6.7.2.2 Checking host communication across EMSn

1 Check the DNS by executing nslookup < local_host> and nslookup <other host>.

2 Check the host route table using netstat -rn.

3 Check the health of the FDDI switch by logging into it, goto FDDI subsystem, and execute smtmib. Look at the health of the interfaces.

4 Run traceroute <target host ip address> or similar tool to discover which router or local route table is in error or not having sufficient route information.

5 Check the Route Advertisement diagram, ECS Connectivity Matrix, and the Network Security Design to see that the filters are not blocking communications or provide no path between hosts. Details are in the configuration of the ECS router. Also check host TCP Wrappers.

6.7.3 Specific Security Limitations

In addition to limiting network access as described above, access is further limited by port level filters installed in the ECS router. In addition to the port filters, a host's tcp wrappers will further limit network access.

Note: Any service that is not listed below is an allowable service.

The following services are NOT permitted in a DAAC's Production and User networks:

1. Remote login (tcp port 513)
2. Remote shell (tcp port 514)
3. Telnet to hosts (tcp port 23)
4. NFS (udp and tcp ports 2049)
5. Port Mapper [RPC] (udp and tcp ports 111)
6. Access to udp and tcp ports 255-1023 on NIS servers
7. X-11[1] (udp and tcp ports 6000-6003)

Each DAAC has its own M&O network. Hosts attached to this network are NOT permitted to use the following services when communicating with their Production and Ingest networks:

1. Remote login (tcp port 513)
2. Remote shell TCP port 514)
3. Telnet (tcp port 23)
4. NFS (udp and tcp ports 2049)
5. Port Mapper [RPC] (udp and tcp ports 111)
6. Access to udp and tcp ports 255-1023 on NIS servers

Note: All other services, including X-11 (udp and tcp ports 6000-6003) are permitted.

Each DAAC has a unique security approach and policy. Details are not provided here because of security considerations.

6.8 Route Add Scripts

On each host which is attached to the Production network, special route add scripts are run at system startup to add several static routes to the host's routing table.

[1] X-11 is a special case. By default it is not allowed for X servers (X-terminals). However, a DAAC can decide to allow X-11 access between a selected set of hosts within the DAAC and an external entity such as a remote SSI&T host or a host at another DAAC. This access would be granted by modifying the appropriate router filter tables.

6.8.1 Script Locations

There is a separate route add script for each host type (Sun, SGI). The scripts are located in the following directories:

- Sun:
  - script S87route_add is in directory /etc/rc2.d.
- SGI:
  - script S87route_add is in directory /etc/init.d with a soft link to /etc/rc2.d/S87route_add.

7. System Monitoring

This chapter covers procedures for the management operations that monitor the network and ECS server applications. Graphical tools available to monitor ECS status include a COTS program, **WhatsUp Gold**, three ECS programs, **ECS Health Check GUI**, **ECS Assistant/ECS Monitor** and **EcMs-Whazzup??**, and a script **EcCsIdPingServers** that permits an operator to ping all servers. These programs provide system monitors with real-time status of the system and indications of potential problem areas. Following this introduction, sections related to System Monitoring address procedures for the following functions:

• Section 7.1	Checking the Health and Status of the Network.
• Section 7.2	Monitoring and Managing Server Applications.

For each set of functions, an **Activity** Checklist table provides an overview of the tasks to be completed. The outline of the Activity Checklist is as follows:

Column one - ***Order*** shows the order in which tasks could be accomplished.

Column two - ***Role*** lists the Role/Manager/Operator responsible for performing the task.

Column three -***Task*** provides a brief explanation of the task.

Column four - ***Section*** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - ***Complete?*** is used as a checklist to keep track of which task steps have been completed.

7.1 Checking the Health and Status of the Network

WhatsUp Gold (Version 8.0) is a graphical network monitoring application selected to monitor critical devices and services on the ECS Production Local Area Network (LAN) and/or additional ECS networks. It initiates alerts when it detects problems, and can send remote notifications by beeper, pager, and e-mail. It logs events to facilitate troubleshooting and reporting. It is implemented on Windows 2000 on a Personal Computer (PC) connected to the Production LAN. Detailed configuration and installation instructions are available in Document 914-TDA-246 *WhatsUp Gold 8.0 for the ECS Project, Release Notes*, and in the following vendor documents:

- *WhatsUp Gold version 8.0 User's Guide and Release Notes* accessible on the internet and downloadable at http://support.ipswitch.com/kb/WG-20030121-DM01.htm

The procedures in this section assume that the installation procedure specified in Document 914-TDA-246 has been executed. The specified procedure installs the WhatsUp Gold 8.0 application, creates a network map, sets up network map alert notifications, sets up a WinPopup notification message, sets up an SMTP e-mail notification message, sets the network map polling properties, sets device properties, saves the map, and starts WhatsUp Gold polling.

Once a network has been discovered by **WhatsUp Gold,** monitoring the state of the network can begin. Monitoring includes tasks such as checking the map for color alerts that indicate problems and checking for network changes.

The **ECS Health Check GUI** indicates the status of the EcDmV0ToEcsGateway and Data Pool. It sends inventory searches to the EcDmV0ToEcsGateway/Data Pool at a specified rate and provides warnings when a failure is registered by the GUI during the current inventory search.

Table 7.1-1 provides an Activity Checklist for checking the health and status of the network.

Table 7.1-1. Checking the Health and Status of the Network - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Administrator/Operations Controller	Launching WhatsUp Gold and Displaying the Network Map	(P) 7.1.1	
2	System Administrator/Operations Controller	Responding to Color Alerts and Obtaining Status of a Node	(P) 7.1.2	
3	System Administrator/Operations Controller	Configuring a Popup Menu for a Node or Multiple Nodes	(P) 7.1.3	
4	System Administrator/Operations Controller	Using the Net Tools Info Tool to Obtain Information on a Node	(P) 7.1.4.1	
5	System Administrator/Operations Controller	Using the Net Tools Ping Tool to Verify Connectivity on a Node	(P) 7.1.4.2	
6	System Administrator/Operations Controller	Using the Net Tools Traceroute Tool to Trace a Route	(P) 7.1.4.3	
7	System Administrator/Operations Controller	Reviewing the WhatsUp Gold Event Log	(P) 7.1.5.1	
8	System Administrator/Operations Controller	Starting and Using the ECS Health Check GUI	(P) 7.1.6	

7.1.1 Launching WhatsUp Gold and Displaying the Network Map

The WhatsUp Gold application and graphical user interface (GUI) are installed and run in the Windows environment on a PC. Once the application is started and being used to monitor the network, it is typically left running at all times. This is because the application must be running with the network map open in order for its monitoring activities (i.e., polling and logging) to occur. Therefore, under normal circumstances, it will seldom be necessary to launch the application because it will be running continually. However, if something causes the application to be stopped (e.g., a failure of its host, or an inadvertent closure of the application), it will be necessary to start it again. Table 7.1-2 presents the steps required to start the WhatsUp Gold application. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Execute the WhatsUpG.exe application in the Windows environment (e.g., double click on the **WhatsUpG** listing in a Windows Explorer window, or click on the **Start** button in the Windows taskbar and then click on the **Run . . .** option to open the **Run** dialog, from which you then enter the path for the **WhatsUpG.exe** application. A typical path is **c:\Program Files\WhatsUp\WhatsUpG.exe**, which may be entered or selected by clicking on the **Browse** button and navigating to the path. When the path is displayed in the **Open:** field of the **Run** dialog, click on the **OK** button.).

- The **WhatsUp Gold** window is opened.

2 Follow menu path **File→Open . . . .**

- The **Open** dialog box is displayed.

3 Double click on the name of your network map, or select the name with a single click and then click on the **Open** button.

- The network map is displayed and polling begins.

Table 7.1-2. Launching WhatsUp Gold and Displaying the Network Map

Step	What to Do	Action to Take
1	Execute **WhatsUpG.exe**	**double-click** or run command
2	**File→Open . . .**	**single-click**
3	Select the name of the network map and display the map	**double-click** or **click** on the name and then on the **Open** button

7.1.2 Responding to Color Alerts and Obtaining Status of a Node

Objects that have an abnormal condition can be identified by a change in appearance on the network map. Colors may be changed, but the following default conventions apply in a map window to indicate the status of a device or service:

- Device name highlighted: indicates that WhatsUp Gold has recorded an event for the device in a log.
- Device icon on a green square background: indicates that the device is up (i.e., responds to polling).
- Device icon on a light green diamond-shaped background: indicates that the device has missed at least one polling request.
- Device icon on a yellow diamond-shaped background: indicates that the device has missed two polling requests.
- Device icon on a red elongated diamond-shaped background: indicates that the device is down (i.e., is not accessible or has missed four consecutive polling requests). Once the device has missed eight polling requests, the background is changed to a dark red starburst.
- Device icon on a light purple octagon-shaped background: indicates that a standard service on the device is down.
- Device on a gray square background: indicates monitoring has been turned off for the device.

A color alert on a symbol indicates that some part of that object may have problems. To help isolate a fault on the network, it is possible to click with the right (or non-preferred) mouse button on the symbol with the color alert and bring up a status display that provides the overall status of the node based on TCP/IP polling, the Internet Control Message Protocol (ICMP) status, and the status of services on the node.

Table 7.1-3 presents the steps required to respond to color alerts and obtain the status of a node. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 With the network map open, use the right (or non-preferred) mouse button to click on the icon for the node showing a color alert (i.e., the node label is highlighted if there has been an entry in the Event Log related to the alert and the background is other than a green square or whatever you have selected as the indication for normal status).

- A popup menu is displayed.

2 On the popup menu, click on **Quick Status . . .**.

- The **Quick Status** dialog box for the selected node is displayed showing the **Status** (including a device status code of 0 to indicate that the device is up or other value to indicate an error, the text of an error message, and information about device polling, ICMP status, and a graph showing any monitored services in green if they are up or red if they are down) and providing access to charts of polling **History** and **Up-Time**. It also provides access to a **Log** display of any service or device "up" or "down" events for the selected node.

3 Review the status information and, in the left frame, click as desired on **History**, **Up-Time**, **Log**, or **Status** to display or re-display information in those categories.

4 Click on the **OK** button to dismiss the **Quick Status** dialog.
- The **Quick Status** dialog is closed.

5 To acknowledge the alert, follow menu path **Monitor→Acknowledge**.
- The highlighting is removed from the node label and additional instances of the alert on the node are prevented (unless the alert has been configured to be sent regardless of the acknowledgement – see **User's Guide**).

Table 7.1-3. Responding to Color Alerts and Obtaining the Status of a Node

Step	What to Do	Action to Take
1	Display the popup menu for a node with an alert	**(non-preferred) click**
2	Open **Quick Status** dialog	**single-click**
3	Review status and related information	**read text, interpret graphs, click(s)**
4	Activate the **OK** button to dismiss **Quick Status** dialog	**single-click**
5	**Monitor→Acknowledge**	**single-click**

7.1.3 Configuring a Popup Menu for a Node or Multiple Nodes

The popup menu accessible using the right (or non-preferred) mouse button to click on a node on a network map typically includes the following choices:

- **Check Now** – initiate a single poll of the network.
- **1 Connect** – open a telnet session on the device represented by the node on the map.
- **2 Ping** – start the Ping tool to send ICMP packets to the device and view the results.
- **3 Traceroute** – start the Traceroute tool to examine the network path and the intervening routers from the WhatsUp Gold machine to the device.
- **4 Browse** – start the default browser using the IP address as the URL.
- **Customize Menu . . .** – open the **Item Properties** dialog box to permit adding, editing, deleting, or moving items on the popup menu.
- **Performance Graphs** – open **Report Job Properties** and **WhatsUp Gold Performance Graphs** dialogs to permit selecting and preparing performance reports and graphs.

- **SNMP View . . .** – start the SNMP View tool using the device's IP address. The SNMP View tool lets you read SNMP data on the device. This command appears only if the SNMP Manageable option (on the Device Properties (SNMP)) is selected.
- **Quick Status . . .** – open the **Quick Status** dialog to provide access to status, history, up-time, and log information for the device.
- **Properties . . .** – open the **Item Properties** dialog box to permit setting parameters for the device, including General functions, monitoring functions, services, alerts, and other categories (see **User's Guide**).

The popup menu may be configured or customized using the **Item Properties** dialog box. If it is desirable to configure the menu in the same way for multiple nodes, this can be achieved by selecting multiple nodes to be configured at the same time. Table 7.1-4 presents the steps required to configure the popup menu for a node or for multiple nodes. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 On the network map, select the node(s) for which the popup menu is to be configured. If more than one node is to be selected, use shift-click (i.e., hold down the shift key and click sequentially on the nodes to be selected) or click-drag (i.e., hold down the mouse button and drag diagonally to outline a rectangle enclosing the items to be selected, releasing the button when the items are enclosed).

- The selected nodes are indicated by the appearance of small white squares at the corners.

2 Use the right (or non-preferred) mouse button to click on the selected node (or one of the selected nodes).

- A popup menu is displayed.

3 On the popup menu, click on **Customize Menu . . .** (for one node) or **Add Custom Menus to Selected Devices . . .** (for multiple nodes).

- If one node was selected, the **Item Properties** dialog box is displayed to permit customization of the menu for that node. (*Note*: It is also possible to display this box for one node by selecting **Properties** from the popup menu and then clicking on **Menu** in the left frame of the resulting **Item Properties** dialog.)
- If more than one node was selected, the **Add to Selected Devices** dialog box is displayed to permit customization of the menus for the selected nodes. This box is similar to the **Item Properties: Menu** dialog, but menu items on any of the selected nodes appear in the dialog box, with a check box next to each item. For an item that is on all selected nodes, the check box is white and displays a check mark; for an item that is assigned to some but not all of the selected nodes, the check box is gray and displays a check mark.

4 To add a menu item, click on the **Add** button.

- The **Edit Menu Item** dialog box is displayed with three empty fields: (1) **Menu name:**; (2) **Command:**; and (3) **Arguments:**. Using this box, it is possible to create a menu item for starting a program when the item is chosen. The Menu name: field is used to specify the name of the menu item that will appear in the popup menu. The Command: field is used to enter the (file)name of any executable program to be started when the menu item is chosen from the popup menu. The Arguments: field is used to pass parameters to the specified program. See the **User's Guide** for detailed information on establishing and using popup menu items to run programs.

5 To select a displayed menu item for editing or moving, click on the menu item in the list.

- The selected item is highlighted.

6 To edit a selected item, click on the **Edit** button.

- The **Edit Menu Item** dialog box is displayed as in Step 4, with information for the selected item displayed in its three fields. The displayed data may be edited to change the menu display and/or actions (see **User's Guide**).

7 To move a selected item up or down in the list, click on the **Move Up** or **Move Down** button as appropriate.

- The selected item is moved up or down in the list as the button is clicked.

8 To delete a selected item for a single node, using the **Item Properties** dialog box, click on the **Delete** button.

- A confirmation dialog is displayed to ensure that you would like to remove the item; click on the **Yes** button to confirm.

9 For multiple nodes, to delete an item from the popup menu for all selected nodes, using the **Add to Selected Devices** dialog, click repeatedly on the accompanying checkbox until the check mark is removed.

- The check box is empty.

10 For multiple nodes, to assign a menu item to all of the selected nodes, using the **Add to Selected Devices** dialog, click repeatedly on the accompanying checkbox until the check mark is displayed in a white (i.e., not gray) box.

- The checkbox is white and the check mark is displayed.

11 Click on the **OK** button.

- The menu changes are applied and the **Item Properties** or **Add to Selected Devices** dialog is closed.

Table 7.1-4. Configuring the Popup Menu for a Node or Multiple Nodes

Step	What to Do	Action to Take
1	Select the node(s) for which the popup menu is to be configured	**single-click** (for single node) or **shift-click** or **click-drag** (for multiple nodes)
2	Display popup menu	**(non-preferred) click**
3	Open **Item Properties** (for single node) or **Add to Selected Devices** dialog box	**single-click**
4	To add a menu item, activate the **Add** button	**single-click**
5	To select a displayed item for editing or moving, highlight the item in the list	**single-click**
6	To edit a selected item, activate the **Edit** button	**single-click**
7	To move a selected item up or down, activate the **Move Up** or **Move Down** button	**click(s)**
8	To delete a selected item for a single node, activate the **Delete** button	**single-click**
9	For multiple nodes, to delete an item, toggle the checkbox to remove the check mark	**click(s)**
10	For multiple nodes, to assign a menu item to all selected nodes, toggle the checkbox to display the check mark in a white box	**click(s)**
11	Activate the **OK** button	**single-click**

7.1.4 Using Network Tools

WhatsUp Gold provides a set of tools to display a variety of information about nodes on the network. These tools are displayed on tabs, with the parameters and results area for one tool on each tab. The tools include:

- **Info** – display a summary of device information.
- **Time** – synchronize your computer's clock with a remote time server.
- **HTML** – query a web address.
- **Ping** – verify connectivity to a host.
- **TraceRoute** – Trace and view the route to an Internet host.
- **Lookup** – query Internet domain name servers for information about hosts and name servers.
- **Finger** – display information about users on a host.
- **Whois** – display information from the network information center about Internet domain ownership and Internet groups.
- **LDAP** – (Lightweight Directory Access Protocol); search directories for names and information stored in an LDAP directory on another computer.
- **Quote** – view quotations from a quote server.

- **Scan** – scan a range of IP addresses to create a network map.
- **SNMP** – view and graph Simple Network Management Protocol (SNMP) values for a device.
- **WinNet** – View Windows Network domains, hosts, and workstations.
- **Throughput** – test data throughput on the connection between your computer and a remote computer.
- **System Info** – view information about your local system.

Not all of these tools will necessarily be appropriate for ECS use, but the **User's Guide** provides detailed information on all of them. Procedures for three of these useful tools are provided here.

7.1.4.1 Using the Net Tools Info Tool to Obtain Information on a Node

The **Info** tool displays a summary of information about a network host or device, including the official host name, IP address, and contact information. An Info request on a host name also pings the host to verify connectivity. Table 7.1-5 presents the steps required to use the Net Tools Info Tool to obtain information on a node. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Follow menu path **Tools→Net Tools. . ..**
- The **Net Tools** window is displayed.

2 If necessary, click on the **Info** tab to access the **Info** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
- The **Info** tab controls and fields are displayed.

3 In the **Host Name or IP Address:** field, type the name or IP address of the host to be queried (this must be a fully qualified host name or address).
- The typed entry is displayed in the field.

4 Click on the **Start** button.
- A **Searching . . .** indicator appears and the **Start** button toggles to **Stop** to show that the query is in progress. At any time during the query, a click on the **Stop** button stops the query.
- The results of the query are displayed. (A click on the **Clear** button erases the results from the display window.) The **List View/Report View** button permits toggling between the Report View and the List View of the results. The Report View is a summary showing:
  - Official Name.
  - Domain Name.
  - Date the record was created.
  - Date the record was last updated.
  - Date the database was last updated.

- Contact information (from the Whois database).
- IP Addresses and Domain Servers.
- The List View is a detailed list of the obtained information, including the results of the ping and more extensive information on the query.

Table 7.1-5. Using the Net Tools Info Tool to Obtain Information on a Node

Step	What to Do	Action to Take
1	Follow menu path **Tools→Net Tools**	**clicks**
2	Ensure **Info** tab is displayed	**single-click**
3	In the **Host Name or IP Address:** field, type the name or IP address of host to be queried	**enter text**
4	To start the query, activate the **Start** button	**single-click**

7.1.4.2 Using the Net Tools Ping Tool to Verify Connectivity on a Node

The **Ping** tool is a network diagnostic tool used to verify connectivity to a selected system on the network. This tool sends a data packet (an ICMP "echo request") to a remote host and displays the results for each "echo reply." This pinging command also displays the time for a response to arrive in milliseconds, as well as debugging information about the network interface. Multiple instances of the **Ping** tool may be active simultaneously.

The use of the **Ping** tool provides a quick way to verify that a device is not functioning. If the ping operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network. See Section 7.1.5 Checking for Event Notifications to verify event status of the node. If a Fault has occurred see Section 8 on Problem Management and Section 21 on COTS Hardware Maintenance.

Table 7.1-6 presents the steps required to use the Net Tools Ping Tool to verify connectivity on a node. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Follow menu path **Tools→Net Tools. . ..**
- The **Net Tools** window is displayed.

2 If necessary, click on the **Ping** tab to access the **Ping** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
- The **Ping** tab controls and fields are displayed.

3 In the **Host Name or IP Address:** field, type the name or IP address of the host to be checked (this must be a fully qualified host name or address).
- The typed entry is displayed in the field.

4 Click one of the radio buttons below the **Host Name or IP Address:** field to specify the protocol to use for pinging (use **ICMP** for TCP/IP hosts, **IPX** for Novell NetWare hosts, or **NetBEUI** for Windows network hosts).

- The selected radio button is filled to indicate the specified protocol.
- *Note*: To ping an IPX device, Microsoft's NWLink IPX/SPX Compatible Transport must be installed and running on the WhatsUp Gold system (see "System Requirements" in the **User's Guide**).

5 If it is desired to change the default number of pings to be sent, click at the end of the **Count:** field.

- The cursor is displayed at the end of the **Count:** field.

6 To set a new value for **Count:**, use the **Backspace** key to remove the current value, and type the new value.

- The typed value appears in the **Count:** field.

7 Repeat Steps 5 and 6 for other options you wish to change, substituting **Delay (sec.):**, **Size**, or **Timeout (ms):** for the field name of the option to be changed, specifying respectively the number of seconds to wait between pings, the length in bytes of each packet to be sent by the **Ping** command, and the number of milliseconds of non-response from the host to be considered a failure of the ping.

8 Click on the **Start** button.

- The **Start** button toggles to **Stop** to show that the ping operation is in progress. At any time during the operation, a click on the **Stop** button stops the pinging.
- The display field at the bottom of the window shows the results of the pings. (A click on the **Clear** button erases the results from the display window.) The **List View/Report View** button permits toggling between the Report View and the List View of the results. The Report View provides, for each ping as it occurs, the address, the number of bytes sent, the response time, and the status. The List View lists the pings, the result for each packet, and the retry code.

Table 7.1-6. Using the Net Tools Ping Tool to Verify Connectivity on a Node (1 of 2)

Step	What to Do	Action to Take
1	Follow menu path **Tools→Net Tools**	**clicks**
2	Ensure **Ping** tab is displayed	**single-click**
3	In the **Host Name or IP Address:** field, type the name or IP address of host to be checked	**enter text**
4	Specify the protocol to use for pinging	**single-click**
5	If it is desired to change the number of pings to be sent, move the cursor to the **Count:** field	**single-click**

Table 7.1-6. Using the Net Tools Ping Tool to Verify Connectivity on a Node (2 of 2)

Step	What to Do	Action to Take
6	To set a new value for **Count:**, type the new value in the field	**enter text**
7	Repeat Steps 5 and 6 for other options to be changed	
8	To initiate the ping(s), activate the **Start** button	**single-click**

7.1.4.3 Using the Net Tools Traceroute Tool to Trace a Route

The **Traceroute** tool permits the operator to trace and view the route an IP packet follows from the local host to another host on the network. Response times are displayed in milliseconds and vary depending on network load. **Traceroute** can be helpful for finding potential trouble spots on large and complex networks that are connected by routers. The results of a traceroute operation can be displayed on a network map.

Table 7.1-7 presents the steps required to use the Net Tools Traceroute Tool to trace a route. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Follow menu path **Tools→Net Tools. . ..**
- The **Net Tools** window is displayed.

2 If necessary, click on the **Traceroute** tab to access the **Traceroute** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
- The **Traceroute** tab controls and fields are displayed.

3 In the **Host Name or IP Address:** field, type the name or IP address of the host to which the route is to be traced (this must be a fully qualified host name or address).
- The typed entry is displayed in the field.

4 If it is desired to change the maximum number of hops to trace before ending the traceroute operation (a “hop” is the passing of an IP packet from one host to another), click at the end of the **Maximum Hopcount:** field.
- The cursor is displayed at the end of the **Maximum Hopcount:** field.

5 To set a new value for **Maximum Hopcount:**, use the **Backspace** key to remove the current value, and type the new value.
- The typed value appears in the **Maximum Hopcount:** field.

6 If it is desired to change the number of milliseconds of non-response from the host to cause the Traceroute to fail, click at the end of the **Timeout (ms):** field.

- The cursor is displayed at the end of the **Timeout (ms):** field.

7 To set a new value for **Timeout (ms):**, use the **Backspace** key to remove the current value, and type the new value.

- The typed value appears in the **Timeout (ms):** field.

8 If it is desired to specify that WhatsUp Gold is to map the results of the Traceroute operation, click on the **Map Results** checkbox.

- The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, the route will be drawn on the network map, displaying an icon for each router and showing the connections from router to router until it reaches the host.

9 If it is desired to specify that the host names of each router along the route are to be displayed along with the IP addresses, click on the **Resolve Addresses** checkbox.

- The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, the host names as well as the IP addresses will be shown for each router (instead of just the IP addresses). This will add time to the Traceroute operation to resolve the IP addresses.

10 If **Map Results** is checked and it is desirable to set dependencies such that each router found is to be set as an "up" dependency on the previous router in the route, click on the **Set Dependencies** checkbox. This choice is only available when **Map Results** is checked. It means that when WhatsUp Gold polling finds a router down, it will not poll routers further along the route to a host.

- The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, each router found will be set as an "up" dependency on the previous router in the route.

11 Click on the **Start** button.

- An indicator shows the Traceroute operation in progress and the **Start** button toggles to **Stop** to show that the operation is in progress. At any time during the operation, a click on the **Stop** button stops the tracing.
- The display field at the bottom of the window shows the results of the traceroute operation. (A click on the **Clear** button erases the results from the display window.) The **List View**/**Report View** button permits toggling between the Report View and the List View of the results. The Report View provides for each hop as it occurs the address, the response time or Round Trip Time (RTT), and the status. The List View lists the hops, addresses, and more detailed information on the tracing of the route.

Table 7.1-7. Using the Net Tools Traceroute Tool to Trace a Route

Step	What to Do	Action to Take
1	Follow menu path **Tools→Net Tools**	**clicks**
2	Ensure **Traceroute** tab is displayed	**single-click**
3	In the **Host Name or IP Address:** field, type the name or IP address of host to which the route is to be traced	**enter text**
4	If it is desired to change the maximum number of hops to trace before ending the traceroute operation, move the cursor to the **Maximum Hopcount:** field	**single-click**
5	To set a new value for **Maximum Hopcount:**, type the new value in the field	**enter text**
6	If it is desired to change the number of milliseconds of non-response from the host to cause the Traceroute to fail, move the cursor to the **Timeout (ms):** field	**single-click**
7	To set a new value for **Timeout (ms):**, type the new value in the field	**enter text**
8	If a map of the Traceroute results is desired, select **Map Results**	**single-click**
9	If router names are desired in the Traceroute results, select **Resolve Addresses**	**single-click**
10	If **Map Results** is selected and router dependencies are desired, select **Set Dependencies**	**single-click**
11	To initiate the Traceroute operation, activate the **Start** button	**single-click**

7.1.5 Using WhatsUp Gold Logs

WhatsUp Gold captures data in four types of logs:

- **Syslog** – logs standard UDP messages sent from devices (e.g., routers, switches, UNIX hosts).
- **Event Log** – logs events (changes to network status, such as a device going down or a device coming back up). The Event Log provides a history of what has occurred on the network. An associated **Debug Log** window permits viewing events as they occur.
- **Statistics Log** – records polling statistics (accumulated round trip times, or RTT, of polls sent to a device) to measure the availability and performance of a device.
- **SNMP Trap Log** – displays all SNMP traps that have been received. To enable SNMP traps, the SNMP trap handler must be specifically enabled (refer to **User's Guide**).

Detailed information on the nature of the logged data and the log designations is provided in the **User's Guide**. The **User's Guide** also describes how to change the way events are logged, and how to create reports and graphs using the logged data to show the status of the network in several ways (e.g., performance graphs, event reports, and statistics reports. Only reviewing of the Event Log is described here, because of its potential utility in troubleshooting.

7.1.5.1 Reviewing the WhatsUp Gold Event Log

The Event Log stores data in weekly file increments with the following file format: **EV-yyyy-mm-dd.tab**. The log automatically records application-level events (e.g., a device or service going down) for devices that have **Enable Logging** selected in the **Alerts** dialog box. After sufficient event data logging, the data can be used to generate reports. The data can also be saved in a tab-delimited file that can be imported to another application, such as a spreadsheet program. It may also be useful just to view the Event Log for information related to an observed problem. For example, if the network map shows a color alert for a device (see Section 7.1.2) and the device does not respond to a ping (see Section 7.1.4.2), the Event Log may provide additional information concerning the time the device went down and a message addressing the problem.

Table 7.1-8 presents the steps required for reviewing the WhatsUp Gold Event Log. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Follow menu path **Logs→Event Log . . .**.

- The **Event Logs - <*date range*>** window is displayed. ***Note***: The date range is the current week, and the events are displayed in raw format (the **Raw** radio button is filled to indicate its selection) with the most recent first. It is possible to click on the **Formatted** radio button to select a display showing the date and time information in *mm/dd/yyyy* and *hh:mm:ss* format, with column headers that can be clicked to sort the list by date, time, or message.

2 Review the list of events to locate a message identifying an **Alert** or **DOWN** event for any device that has shown a color alert on the network map or that has failed to respond to pinging.

- The message provides the date and time of the event, as well as specific information in the message concerning the type of event.

3 If it is desirable to view events from the prior week, click on the **Back** icon (⇦).

- The events from the previous week are displayed. ***Note***: The date range specifies the prior week, and the events are displayed in the currently selected format (raw or formatted) with the most recent first. There are other icons: a **Filter** icon (or menu equivalent) permits customizing the log viewer to show logs in a different time span other than weekly; a **Find** icon permits locating text in the display; a **Print** icon permits printing the contents of the display; and other navigation icons permit moving to specific ranges of events for display. The **User's Guide** provides detailed guidance on navigating and locating text in the Event Log display.

4 If it is desirable to print the contents of the display, click on the **Print** icon.

- The **Print** dialog box is displayed, permitting specification of a printer, print range, and number of copies.

Table 7.1-8. Reviewing the WhatsUp Gold Event Log

Step	What to Do	Action to Take
1	Follow menu path **Logs→Event Logs**	**clicks**
2	Review list of events for suspect device	**read text**
3	If it is desired to view events from other than the current week, activate the **Back** icon button or other navigation button	**click(s)**
4	If it is desired to print the contents of the display, activate the **Print** icon button and, in the resulting dialog, specify print options	**clicks**

7.1.6 Starting and Using the ECS Health Check GUI

The **ECS Health Check GUI** indicates the status of the EcDmV0ToEcsGateway and Data Pool. It sends inventory searches to the EcDmV0ToEcsGateway/Data Pool at a specified rate and provides warnings by the following means when a failure is registered by the GUI during the current inventory search:

- Visual warning (including details about the time and nature of the error).
- Audible alarm (when implemented).
- E-mail message.

Table 7.1-9 presents the steps required for starting and using the ECS Health Check GUI. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Log in to the Sun Consolidation Internal Server host.

- Examples of Sun Consolidation Internal Server hosts include **g0acs11**, **e0acs11**, **l0acs03**, and **n0acs04**.
- For detailed instructions refer to the **Log in to ECS** procedure (previous section of this lesson).

2 At the UNIX prompt type **cd /usr/ecs/<*MODE*>/CUSTOM/bin/CSS** and then press the **Return/Enter** key.

- Change to the directory containing the start script (i.e., EcCsHealthCheckStart) for the ECS Health Check GUI.

3 At the UNIX prompt type **EcCsHealthCheckStart <*MODE*>** and then press the **Return/Enter** key.

- The ECS Health Check GUI is displayed.

4 Click on the appropriate tab for the area to be monitored.

- The following choices are available:
  - **EcDmV0ToEcsGateway.**
  - **ECS Datapools.**

5 In the **Specify timeout period minutes** and **seconds** text entry boxes type the number of minutes and seconds (respectively) before timeout.

- **Timeout period** specifies how long the GUI will wait for a response from the current search before flagging an error.

6 In the **Specify repeat period minutes** and **seconds** text entry boxes type the number of minutes and seconds (respectively) before repeating a search.

- **Repeat period** specifies how often the GUI sends an inventory search to the area being monitored.

7 Click on the **Start** button in the **Control** pane to start checking the selected area.

- The ECS Health Check GUI starts sending inventory searches to the selected area at the frequency specified in the **Specify repeat period** text boxes.
- **The Current Status is:** (as displayed on the GUI) changes from **Dormant** to **Running**.

8 Repeat Steps 4 through 7 to set up inventory searches of the other area (if applicable).

9 Observe information displayed in the **Visual Warnings** pane of the ECS Health Check GUI and listen for audible warnings (if enabled).

- Nothing much will appear to happen unless an error occurs in an inventory search sent to the EcDmV0ToEcsGateway/Data Pool, in which case the following indications will be evident:
  - **The Current Status is:** (as displayed on the GUI) changes from **Running** to **Failed** (in red).
  - Details concerning the time and nature of the error are displayed in the **Visual Warnings** text pane.
  - The **Mail Warnings** pane indicates that mail has been sent successfully to the recipients in the list.
  - A repeating audible alarm sounds (if enabled).
- If an error occurs in an inventory search sent to the EcDmV0ToEcsGateway/Data Pool, no further inventory searches will be sent to the selected area unless restarted using the **Start** button in the **Control** pane (refer to Step 13).

10 To stop an audible alarm (when applicable) click on the **Stop** button in the **Audible Warnings** pane.

- The alarm stops sounding.

11 To clear error information from the ECS Health Check GUI (when applicable) click on the **Reset** button in the **Control** pane.

- The error information is cleared from the ECS Health Check GUI.

12 To stop inventory searches of the selected area, (when applicable) click on the **Stop** button in the **Control** pane.

- The GUI goes to a dormant state.

13 To restart inventory searches of the selected area, (when applicable) return to Step 7 (click on the **Start** button in the **Control** pane).

- The GUI goes to a dormant state.

14 To exit from the ECS Health Check GUI (when applicable) select **File → Exit** from the pull-down menu.

- The ECS Health Check GUI is dismissed.

Table 7.1-9. Starting and Using the ECS Health Check GUI

Step	What to Do	Action to Take
1	Log in to the Sun Consolidation Internal Server host	
2	**cd /usr/ecs/<*MODE*>/CUSTOM/bin/CSS**	**enter text; press Return/Enter**
3	**EcCsHealthCheckStart <*MODE*>**	**enter text; press Return/Enter**
4	**EcDmV0ToEcsGateway** or **ECS Datapools** tab (as applicable)	**single-click**
5	***minutes/seconds*** (in the **Specify timeout period minutes** and **seconds** text entry boxes)	**enter text**
6	***minutes/seconds*** (in the **Specify repeat period minutes** and **seconds** text entry boxes)	**enter text**
7	**Start** button (in the **Control** pane)	**single-click**
8	Repeat Steps 4 through 7 (if applicable).	
9	Observe information displayed in the **Visual Warnings** pane of the ECS Health Check GUI and listen for audible warnings (if enabled)	**read text; listen for sound**
10	**Stop** button (in the **Audible Warnings** pane) (when applicable)	**single-click**
11	**Reset** button (in the **Control** pane) (when applicable)	**single-click**
12	**Stop** button (in the **Control** pane) (when applicable)	**single-click**
13	Return to Step 7 (to restart inventory searches of the selected area) (when applicable)	
14	**File** → **Exit** (when applicable)	**single-click**

7.2 Monitoring and Managing Server Applications

There are two applications and an accompanying script provided as part of ECS for monitoring and managing server applications. **Whazzup???** is a management tool that provides operators and maintainers with a means of monitoring and checking servers, for quickly identifying servers that may have problems, and for isolating faults. It is a web-based application, and is therefore accessed by means of browser software. It provides the following general features:

- host and mode views of network resources.
- status information on resources (indicated by color coding: purple indicates inability to ping the specified host, blue indicates incomplete data collection, red indicates that the server is down, and yellow indicates that a warning threshold has been exceeded).
- performance monitoring capability.

Another set of tools for monitoring and managing system resources is **ECS Assistant** and its companion, **ECS Monitor**, which offer:

- installation support.
- indication of network and server status and changes.

There is an accompanying script, **EcCsIdPingServers**, which provides the capability to ping all servers.

Table 7.2-1 provides an Activity Checklist for monitoring and managing server applications.

Table 7.2-1. Monitoring and Managing Server Applications - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Administrator/Operations Controller	Launching EcMs-Whazzup?? and Determining What’s Down	(P) 7.2.1	
2	System Administrator/Operations Controller	Starting ECS Assistant	(P) 7.2.2.1	
3	System Administrator/Operations Controller	Starting ECS Monitor	(P) 7.2.2.2	
4	System Administrator/Operations Controller	Using EcCsIdPingServers to Ping All Servers in a Mode	(P) 7.2.2.3	

7.2.1 Launching EcMs-Whazzup?? and Determining What's Down

A powerful COTS program that has been modified for ECS and used to monitor the ECS system is EcMsWz-Whazzup??. It is a web-accessed program that provides a graphical display of Host Status, Mode Status, Mode Verification and Performance Management. The welcome screen has buttons and links at the bottom permitting an operator to view status by various means (e.g., host, mode), verify modes and view what servers may be down, and access data on performance. The **Performance Stats** screen provides a quick overview of the system status; if Whazzup is unable to ping a host, the row for that host is highlighted in purple.

These functions of Whazzup?? provide graphical displays of host and software-server status in real-time mode. When used in conjunction with WhatsUp Gold and ECS Assistant, Whazzup?? can provide System Administrators with a comprehensive knowledge of the system's status.

Table 7.2-2 presents the steps required for launching Whazzup?? and determining what's down. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 On workstation ***x*0ins02**, at the UNIX prompt in a terminal window, type **netscape &** and then press the **Return/Enter** key.

- **NOTE:** The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL (e.g., **l0ins02** indicates an interface host workstation at LaRC).

2 In the location field, type **http://*x*0ins02u:5150** and press the **Return/Enter** key.

- The **EcMsWz-Whazzup???** screen is displayed.

3 At the bottom of the screen, click on the **Verify Mode** option button and, in the resulting pop-up menu, drag the cursor to highlight the option **What's Down**.

- The screen displays a table showing **Required Servers Currently Down . . .**, listing by mode the servers that are down.

4 Move the mouse to position the cursor on the **Performance** link, click the **Right Mouse Button**, and select **Open Link in New Window**.

- The **Performance Stats** screen is displayed in a new window, showing information that may help determine the reason for any servers being down.

5 If desired, click on the link for any host to obtain more detailed information.

- An information screen for the selected host is displayed, showing data on system memory, disk utilization, process information, and network information.

Table 7.2-2. Launching Whazzup?? and Determining What's Down

Step	What to Do	Action to Take
1	At the UNIX prompt, enter **netscape &**	**enter text; press Return/Enter**
2	Enter **http://x0ins02u:5150** in the location field	**enter text; press Return/Enter**
3	Use the **Verify Mode** option button to select **What's Down**	**click-drag**
4	Use right (or non-preferred) mouse button and the **Performance** link to open the **Performance Stats** screen in a new window	**(non-preferred) click; click**
5	If desired, use the link for any host to display more detailed information	**click**

7.2.2 ECS Assistant and ECS Monitor

The Whazzup tool provides a quick look capability to note whether any servers are down. The ECS Assistant and ECS Monitor tools provide additional easy-to-use tools that offer a server monitoring capability (ECS Monitor) as well as a capability to start and stop servers (ECS Assistant).

7.2.2.1 Starting ECS Assistant

Table 7.2-3 presents the steps required for starting ECS Assistant. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Log in to one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, and then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME**, and then press the **Return/Enter** key.

3 At the UNIX prompt, type **cd /tools/common/ea**, and then press the **Return/Enter** key.

- The working directory is changed to **/tools/common/ea**, the path where ECS Assistant is installed, and also where EcCoScriptlib may be found.

4 Type **EcCoAssist /tools/common/ea &**, and then press the **Return/Enter** key.

- The **ECS Assistant** GUI is displayed.

5 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- The **Subsystem Manager** GUI is displayed.

6 Select a mode by clicking on the down arrow at the right end of the **Mode** field and then on the desired mode name in the resulting list.

- The selected mode is displayed in the **Mode** field and colored indicators show the installation status for components in that mode on the host; the legend for the color indications is at the lower right on the Subsystem Manager window.

7 In the list of subsystems, double click on the name of the subsystem of interest.

- One or more component groups appear below the selected subsystem name.

8 Double click on the name of a component group.

- One or more application groups appear below the selected component group name.

9 Double click on the name of the application group of interest.

- The applications or servers in the selected group are listed below the name of the group.

10 Single click on the name of an application or server of interest.

- The selected application or server is highlighted.
- Detailed installation information is displayed in the **Installation Statistics** window.

Table 7.2-3. Starting ECS Assistant

Step	What to Do	Action to Take
1	Log into one of the host machines	
2	**setenv ECS_HOME /usr/ecs**	**enter text; press Return/Enter**
3	**cd /tools/common/ea**	**enter text; press Return/Enter**
4	**EcCoAssist /tools/common/ea &** (starts the GUI)	**enter text; press Return/Enter**
5	Activate the **Subsystem Manager** pushbutton	**single-click**
6	Use the down arrow at the right end of the **Mode** field to select the desired mode	**clicks**
7	From the listed subsystems, display the component groups for the subsystem of interest	**double-click** subsystem name
8	From the listed component groups, display the application groups for any component group of interest	**double-click** component group name
9	From the listed application groups, display the applications or servers for any application group of interest	**double-click** application group name
10	From the list of applications or servers, select an application or server and display detailed information concerning its installation	**single-click** application or server name

7.2.2.2 Starting ECS Monitor

ECS Monitor provides a convenient way to monitor the status of the servers by listing their up/down condition. The **ECS Monitor** GUI has a status flag for a server indicating whether or not that server is running, and for a server that is running, the window shows the process ID (PID), the user ID, and the start time.

Table 7.2-4 presents the steps required for starting ECS Monitor. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Log in to one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, and then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME**, and then press the **Return/Enter** key.

3 At the UNIX prompt, type **cd /tools/common/ea**, and then press the **Return/Enter** key.

- The working directory is changed to **/tools/common/ea**, the path where ECS Monitor is installed, and also where EcCoScriptlib may be found.

4 Type **EcCoMonitorGui /tools/common/ea <*MODE*> &**, and then press the **Return/Enter** key.

- The **ECS Monitor GUI** is displayed, showing the status (**UP** or **DOWN**) of the servers on the current host in the mode specified in the command, as indicated near the top left corner of the window.
- The status "**UP/DOWN**" indicates whether a listed server is running.

5 To update the **Server Monitor** to show the current status at any time, click on the **update** button in the GUI.

- This causes the list to update to the current status.

6 To monitor other servers, log in to other hosts and launch the ECS Monitor GUI in the desired mode, as in Steps 1 through 4.

7 To exit, click the **EXIT** button.

- This terminates display of the ECS Monitor GUI.

Table 7.2-4. Starting ECS Monitor

Step	What to Do	Action to Take
1	Log into one of the host machines	
2	**setenv ECS_HOME /usr/ecs**	**enter text; press Return/Enter**
3	**cd /tools/common/ea**	**enter text; press Return/Enter**
4	**EcCoMonitorGui /tools/common/ea <*MODE*>&** (starts the GUI to monitor the specified mode)	**enter text; press Return/Enter**
5	To update to the current status at any time, activate the **Update** button	**single-click**
6	To monitor other servers, repeat Steps 1 through 4 for other hosts their servers	
7	To exit, activate the **EXIT** button	**single-click**

7.2.2.3 Using EcCsIdPingServers to Ping All Servers in a Mode

The script **EcCsIdPingServers** script works with a *Sweeper* binary to ping the servers and clients in a mode to determine their status. Table 7.2-5 presents the steps required for using EcCsIdPingServers to ping all servers in a mode. If you are already familiar with the procedure, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the following detailed procedure:

1 Log in to one of the host machines.

2 At the UNIX prompt, type **cd /usr/ecs/<*MODE*>/CUSTOM/utilities**, and then press the **Return/Enter** key.

- The prompt reflects a change to directory **cd /usr/ecs/<*MODE*>/CUSTOM/utilities**, where **<*MODE*>** is likely to be **OPS**, **TS1**, or **TS2**.

3 Then type **EcCsIdPingServers <*MODE*>**, and then press the **Return/Enter** key.

- The result should appear similar to the following:

```
/usr/ecs/DEV03/CUSTOM/bin/CSS/Sweeper -nsh dss2 -nsp 22822
FoSwSweeper application started...
We made a connection with EntryId =g0icg01:17871:12451240 ---
EcSrTransportEcInGranServer
We made a connection with EntryId =g0ins02:22336:6737528 --- DsHrQuitIDL
We made a connection with EntryId =g0pls02:35211:25637 --- PlOdMsgDObj
We made a connection with EntryId =g0dis02:48315:18311 --- DsDdRequestMgrIDL
We made a connection with EntryId = g0ins02:17862:12461267 --- InAutoIngestIF
We made a connection with EntryId = g0dis02:49473:13375 --- DsStReqMgrIDL
We made a connection with EntryId = g0ins02:41566:13071 --- IoAdRpc
We made a connection with EntryId = g0ins02:18139:12460808 --- InRequestMgrIF
We made a connection with EntryId =g0dms03:42000:13266 --- EcSrTransportDDICT
We made a connection with EntryId = g0pls02:22359:6737528 ---
    DsHrNonConfIDL681ab65e-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId = g0pls02:22346:6737528 ---
    DsHrConformantIDL681ab65d-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0mss21:64657:8006 --- EcAcOrderMgr
We made a connection with EntryId =g0mss11:41449:22898 ---
EcSrTransportDarServer
We made a connection with EntryId = g0icg02:17724:12445092 --- EcRgRegistry
We made a connection with EntryId =g0mss11:41278:22739 --- InDDNTransferPkt
We made a connection with EntryId =g0psl02:35085:25466 --- Deletion
We made a connection with EntryId =g0pls02:35168:25584 --- SubscriptionQueue
We made a connection with EntryId =g0mss21:64700:8059 --- MsAcUsrRequestMgr
We made a connection with EntryId =g0mss21:64690:8059 --- MsAcRegUserMgr
We made a connection with EntryId =g0mss21:64695:8059 --- MsAcUsrProfileMgr
We made a connection with EntryId =g0pls02:35127:25527 --- DpPrSchedulerDObj
We made a connection with EntryId =g0ins02:22364:6738409 ---
   DsHrNonConfIDL681ab654-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0ins02:22353:6738409 ---
   DsHrConformantIDL681ab653-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0ins02:22342:6738409 --- DsHrQuitIDL
```

Table 7.2-5. Using EcCsIdPingServers to Ping All Servers in a Mode

Step	What to Do	Action to Take
1	Log into one of the host machines	
2	**cd /usr/ecs/<*MODE*>/CUSTOM/utilities**	**enter text; press Return/Enter**
3	**EcCsIdPingServers <*MODE*>**	**enter text; press Return/Enter**

This page intentionally left blank.